Actual exam question from Isaca's CISM

Question #: 1

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 2

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 3

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 4

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 5

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 6

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 7

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 8

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 9

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 10

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 11

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 12

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 13

Topic #: 1

[All CISM Questions]

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)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 14

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 15

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 16

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 17

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 18

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 19

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 20

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 21

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 22

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 23

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 24

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 25

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 26

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 27

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 28

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 29

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 30

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 31

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 32

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 33

Topic #: 1

[All CISM Questions]

An organization has identified an increased threat of external brute force attacks in its environment. Which of the following is the MOST effective way to mitigate this risk to the organization's critical systems?

A. Increase the frequency of log monitoring and analysis.

B. Implement a security information and event management system (SIEM).

C. Increase the sensitivity of intrusion detection systems.

D. Implement multi-factor authentication.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 34

Topic #: 1

[All CISM Questions]

When supporting an organization's privacy officer which of the following is the information security manager's PRIMARY role regarding privacy requirements?

A. Ensuring appropriate controls are in place

B. Monitoring the transfer of private data

C. Determining data classification

D. Conducting privacy awareness programs

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 35

Topic #: 1

[All CISM Questions]

The chief information security officer (CISO) has developed an information security strategy, but is struggling to obtain senior management commitment for funds to implement the strategy. Which of the following is the MOST likely reason?

A. The strategy does not include a cost-benefit analysis.

B. There was a lack of engagement with the business during development.

C. The strategy does not comply with security standards.

D. The CISO reports to the CIO.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 36

Topic #: 1

[All CISM Questions]

An organization's CIO has tasked the information security manager with drafting the charter for an information security steering committee. The committee will be comprised of the CIO, the IT shared services manager, the vice president of marketing, and the information security manager. Which of the following is the MOST significant issue with the development of this committee?

A. The committee consists of too many senior executives.

B. The committee lacks sufficient business representation.

C. There is a conflict of interest between the business and IT.

D. The CIO is not taking charge of the committee.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 37

Topic #: 1

[All CISM Questions]

What is the PRIMARY purpose of an unannounced disaster recovery exercise?

A. To provide metrics to senior management

B. To evaluate how personnel react to the situation

C. To assess service level agreements (SLAs)

D. To estimate the recovery time objective (RTO)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 38

Topic #: 1

[All CISM Questions]

Labeling information according to its security classification:

A. reduces the need to identify baseline controls for each classification.

B. reduces the number and type of countermeasures required.

C. enhances the likelihood of people handling information securely.

D. affects the consequences if information is handled insecurely.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 39

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective approach for determining whether an organization's information security program supports the information security strategy?

A. Ensure resources meet information security program needs

B. Audit the information security program to identify deficiencies

C. Identify gaps impacting information security strategy

D. Develop key performance indicators (KPIs) of information security

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 40

Topic #: 1

[All CISM Questions]

When drafting the corporate privacy statement for a public web site, which of the following MUST be included?

A. Limited liability clause

B. Access control requirements

C. Explanation of information usage

D. Information encryption requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 41

Topic #: 1

[All CISM Questions]

An organization is concerned with the potential for exploitation of vulnerabilities in its server systems. Which of the following is the BEST control to mitigate the associated risk?

A. Enforcing standard system configurations based on secure configuration benchmarks

B. Implementing network and system-based anomaly monitoring software for server systems

C. Enforcing configurations for secure logging and audit trails on server systems

D. Implementing host-based intrusion detection systems (IDS) on server systems

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 42

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important step when establishing guidelines for the use of social networking sites in an organization?

A. Identify secure social networking sites

B. Establish disciplinary actions for noncompliance

C. Perform a vulnerability assessment

D. Define acceptable information for posting

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 43

Topic #: 1

[All CISM Questions]

Regular vulnerability scanning on an organization's internal network has identified that many user workstations have unpatched versions of software. What is the BEST way for the information security manager to help senior management understand the related risk?

A. Include the impact of the risk as part of regular metrics.

B. Send regular notifications directly to senior managers.

C. Recommend the security steering committee conduct a review.

D. Update the risk assessment at regular intervals.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 44

Topic #: 1

[All CISM Questions]

Which of the following BEST prepares a computer incident response team for a variety of information security scenarios?

A. Tabletop exercises

B. Forensics certification

C. Penetration tests

D. Disaster recovery drills

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 45

Topic #: 1

[All CISM Questions]

Which of the following BEST protects against phishing attacks?

A. Security strategy training

B. Email filtering

C. Network encryption

D. Application whitelisting

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 46

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective method of preventing deliberate internal security breaches?

A. Well-designed intrusion detection system (IDS)

B. Biometric security access control

C. Well-designed firewall system

D. Screening prospective employees

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 47

Topic #: 1

[All CISM Questions]

When designing security controls, it is MOST important to:

A. focus on preventive controls.

B. apply controls to confidential information.

C. evaluate the costs associated with the controls.

D. apply a risk-based approach.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 48

Topic #: 1

[All CISM Questions]

An information security team plans to increase password complexity requirements for a customer-facing site, but there are concerns it will negatively impact the user experience. Which of the following is the information security manager's BEST course of action?

A. Evaluate business compensating controls.

B. Quantify the security risk to the business.

C. Assess business impact against security risk.

D. Conduct industry benchmarking.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 49

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY responsibility of an information security manager in an organization that is implementing the use of company-owned mobile devices in its operations?

A. Review and update existing security policies.

B. Enforce passwords and data encryption on the devices.

C. Conduct security awareness training.

D. Require remote wipe capabilities for devices.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 50

Topic #: 1

[All CISM Questions]

Which of the following would be MOST useful to help senior management understand the status of information security compliance?

A. Key performance indicators (KPIs)

B. Risk assessment results

C. Industry benchmarks

D. Business impact analysis (BIA) results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 51

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important reason for an organization to develop an information security governance program?

A. Establishment of accountability

B. Compliance with audit requirements

C. Creation of tactical solutions

D. Monitoring of security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 52

Topic #: 1

[All CISM Questions]

Which of the following provides the MOST essential input for the development of an information security strategy?

A. Results of an information security gap analysis

B. Measurement of security performance against IT goals

C. Results of a technology risk assessment

D. Availability of capable information security resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 53

Topic #: 1

[All CISM Questions]

The MOST important reason for an information security manager to be involved in the change management process is to ensure that:

A. security controls drive technology changes.

B. risks have been evaluated.

C. security controls are updated regularly.

D. potential vulnerabilities are identified.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 54

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY focus of a status report on the information security program to senior management?

A. Confirming the organization complies with security policies

B. Verifying security costs do not exceed the budget

C. Demonstrating risk is managed at the desired level

D. Providing evidence that resources are performing as expected

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 55

Topic #: 1

[All CISM Questions]

Which of the following is MOST likely to be a component of a security incident escalation policy?

A. Names and telephone numbers of key management personnel

B. A severity-ranking mechanism tied only to the duration of the outage

C. Sample scripts and press releases for statements to media

D. Decision criteria for when to alert various groups

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 56

Topic #: 1

[All CISM Questions]

Which of the following would be an information security manager's PRIMARY challenge when deploying a bring your own device (BYOD) mobile program in an enterprise?

A. Configuration management

B. Mobile application control

C. Inconsistent device security

D. End user acceptance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 57

Topic #: 1

[All CISM Questions]

Company A, a cloud service provider, is in the process of acquiring Company B to gain new benefits by incorporating their technologies within its cloud services.
Which of the following should be the PRIMARY focus of Company A's information security manager?

A. The cost to align to Company A's security policies

B. The organizational structure of Company B

C. Company B's security policies

D. Company A's security architecture

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 58

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST when selecting performance metrics to report on the vendor risk management process?

A. Select the data source.

B. Review the confidentiality requirements.

C. Identify the intended audience.

D. Identify the data owner.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 59

Topic #: 1

[All CISM Questions]

Which of the following BEST determines what information should be shared with different entities during incident response?

A. Escalation procedures

B. Communication plan

C. Disaster recovery policy

D. Business continuity plan (BCP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 60

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to enhance training for incident response teams?

A. Conduct interviews with organizational units.

B. Establish incident key performance indicators (KPIs).

C. Participate in emergency response activities.

D. Perform post-incident reviews.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 61

Topic #: 1

[All CISM Questions]

An information security manager wants to improve the ability to identify changes in risk levels affecting the organization's systems. Which of the following is the BEST method to achieve this objective?

A. Performing business impact analyses (BIA)

B. Monitoring key goal indicators (KGIs)

C. Monitoring key risk indicators (KRIs)

D. Updating the risk register

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 62

Topic #: 1

[All CISM Questions]

When developing an escalation process for an incident response plan, the information security manager should PRIMARILY consider the:

A. affected stakeholders.

B. incident response team.

C. availability of technical resources.

D. media coverage

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 63

Topic #: 1

[All CISM Questions]

Which of the following should be an information security managers MOST important consideration when determining if an information asset has been classified appropriately?

A. Value to the business

B. Security policy requirements

C. Ownership of information

D. Level of protection

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 64

Topic #: 1

[All CISM Questions]

The effectiveness of an incident response team will be GREATEST when:

A. the incident response process is updated based on lessons learned.

B. the incident response team members are trained security personnel.

C. the incident response team meets on a regular basis to review log files.

D. incidents are identified using a security information and event monitoring (SIEM) system.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 65

Topic #: 1

[All CISM Questions]

An information security manager MUST have an understanding of the organization's business goals to:

A. relate information security to change management.

B. develop an information security strategy.

C. develop operational procedures

D. define key performance indicators (KPIs).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 66

Topic #: 1

[All CISM Questions]

An information security manager MUST have an understanding of an information security program?

A. Understanding current and emerging technologies

B. Establishing key performance indicators (KPIs)

C. Conducting periodic risk assessments

D. Obtaining stakeholder input

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 67

Topic #: 1

[All CISM Questions]

An attacker was able to gain access to an organization's perimeter firewall and made changes to allow wider external access and to steal data. Which of the following would have BEST provided timely identification of this incident?

A. Implementing a data loss prevention (DLP) suite

B. Deploying an intrusion prevention system (IPS)

C. Deploying a security information and event management system (SIEM)

D. Conducting regular system administrator awareness training

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 68

Topic #: 1

[All CISM Questions]

When establishing metrics for an information security program, the BEST approach is to identify indicators that:

A. support major information security initiatives.

B. reflect the corporate risk culture.

C. reduce information security program spending.

D. demonstrate the effectiveness of the security program.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 69

Topic #: 1

[All CISM Questions]

For an organization that provides web-based services, which of the following security events would MOST likely initiate an incident response plan and be escalated to management?

A. Anti-malware alerts on several employees' workstations

B. Several port scans of the web server

C. Multiple failed login attempts on an employee's workstation

D. Suspicious network traffic originating from the demilitarized zone (DMZ)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 70

Topic #: 1

[All CISM Questions]

An information security manager is implementing a bring your own device (BYOD) program. Which of the following would BEST ensure that users adhere to the security standards?

A. Publish the standards on the intranet landing page.

B. Deploy a device management solution.

C. Establish an acceptable use policy.

D. Monitor user activities on the network.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 71

Topic #: 1

[All CISM Questions]

When monitoring the security of a web-based application, which of the following is MOST frequently reviewed?

A. Audit reports

B. Access logs

C. Access lists

D. Threat metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 72

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way for an information security manager to ensure that security is incorporated into an organization's project development processes?

A. Develop good communications with the project management office (PMO).

B. Participate in project initiation, approval, and funding.

C. Conduct security reviews during design, testing, and implementation.

D. Integrate organization's security requirements into project management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 73

Topic #: 1

[All CISM Questions]

Which of the following provides the MOST relevant information to determine the overall effectiveness of an information security program and underlying business processes?

A. SWOT analysis

B. Industry benchmarks

C. Cost-benefit analysis

D. Balanced scorecard

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 74

Topic #: 1

[All CISM Questions]

An organization finds unauthorized software has been installed on a number of workstations. The software was found to contain a Trojan, which had been uploading data to an unknown external party. Which of the following would have BEST prevented the installation of the unauthorized software?

A. Banning executable file downloads at the Internet firewall

B. Implementing an intrusion detection system (IDS)

C. Implementing application blacklisting

D. Removing local administrator rights

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 75

Topic #: 1

[All CISM Questions]

When developing a tabletop test plan for incident response testing, the PRIMARY purpose of the scenario should be to:

A. measure management engagement as part of an incident response team.

B. provide participants with situations to ensure understanding of their roles.

C. give the business a measure of the organization's overall readiness.

D. challenge the incident response team to solve the problem under pressure.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 76

Topic #: 1

[All CISM Questions]

Which of the following is MOST important for an information security manager to consider when identifying information security resource requirements?

A. Availability of potential resources

B. Information security incidents

C. Current resourcing levels

D. Information security strategy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 77

Topic #: 1

[All CISM Questions]

Which of the following is the MAIN benefit of performing an assessment of existing incident response processes?

A. Validation of current capabilities

B. Benchmarking against industry peers

C. Prioritization of action plans

D. Identification of threats and vulnerabilities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 78

Topic #: 1

[All CISM Questions]

Which of the following BEST describes a buffer overflow?

A. A type of covert channel that captures data

B. A function is carried out with more data than the function can handle

C. Malicious code designed to interfere with normal operations

D. A program contains a hidden and unintended function that presents a security risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 79

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when selecting members for an information security steering committee?

A. Information security expertise

B. Tenure in the organization

C. Business expertise

D. Cross-functional composition

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 80

Topic #: 1

[All CISM Questions]

Which of the following BEST validates that security controls are implemented in a new business process?

A. Verify the use of a recognized control framework

B. Review the process for conformance with information security best practices

C. Benchmark the process against industry practices

D. Assess the process according to information security policy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 81

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way for an organization to ensure its third-party service providers are aware of information security requirements and expectations?

A. Including information security clauses within contracts

B. Auditing the service delivery of third-party providers

C. Providing information security training to third-party personnel

D. Requiring third parties to sign confidentiality agreements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 82

Topic #: 1

[All CISM Questions]

The MOST important reason to use a centralized mechanism to identify information security incidents is to:

A. comply with corporate policies

B. detect threats across environments

C. prevent unauthorized changes to networks

D. detect potential fraud

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 83

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST when establishing security measures for personal data stored and processed on a human resources management system?

A. Conduct a vulnerability assessment.

B. Move the system into a separate network.

C. Conduct a privacy impact assessment (PIA).

D. Evaluate data encryption technologies.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 84

Topic #: 1

[All CISM Questions]

An information security manager has been informed of a new vulnerability in an online banking application, and a patch to resolve this issue is expected to be released in the next 72 hours. Which of the following should the information security manager do FIRST?

A. Implement mitigating controls.

B. Perform a business impact analysis (BIA).

C. Perform a risk assessment.

D. Notify senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 85

Topic #: 1

[All CISM Questions]

Which of the following is MOST relevant for an information security manager to communicate to the board of directors?

A. The level of exposure

B. Vulnerability assessments

C. The level of inherent risk

D. Threat assessments

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 86

Topic #: 1

[All CISM Questions]

Senior management has just accepted the risk of noncompliance with a new regulation. What should the information security manager do NEXT?

A. Report the decision to the compliance officer.

B. Reassess the organization's risk tolerance.

C. Update details within the risk register.

D. Assess the impact of the regulation.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 87

Topic #: 1

[All CISM Questions]

Which of the following BEST provides an information security manager with sufficient assurance that a service provider complies with the organization's information security requirements?

A. A live demonstration of the third-party supplier's security capabilities

B. The ability to audit the third-party supplier's IT systems and processes

C. Third-party security control self-assessment results

D. An independent review report indicating compliance with industry standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 88

Topic #: 1

[All CISM Questions]

Which of the following is the MOST essential element of an information security program?

A. Prioritizing program deliverables based on available resources

B. Benchmarking the program with global standards for relevance

C. Involving functional managers in program development

D. Applying project management practices used by the business

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 89

Topic #: 1

[All CISM Questions]

Which of the following is BEST to include in a business case when the return on investment (ROI) for an information security initiative is difficult to calculate?

A. Projected increase in maturity level

B. Estimated increase in efficiency

C. Projected costs over time

D. Estimated reduction in risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 90

Topic #: 1

[All CISM Questions]

If the inherent risk of a business activity is higher than the acceptable risk level, the information security manager should FIRST:

A. transfer risk to a third party to avoid cost of impact.

B. recommend that management avoid the business activity.

C. assess the gap between current and acceptable level of risk.

D. implement controls to mitigate the risk to an acceptable level.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 91

Topic #: 1

[All CISM Questions]

Which of the following BEST enables the deployment of consistent security throughout international branches within a multinational organization?

A. Remediation of audit findings

B. Decentralization of security governance

C. Establishment of security governance

D. Maturity of security processes

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 92

Topic #: 1

[All CISM Questions]

What is the PRIMARY benefit of effective configuration management?

A. Standardization of system support

B. Reduced frequency of incidents

C. Decreased risk to the organization's systems

D. Improved vulnerability management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 93

Topic #: 1

[All CISM Questions]

A large organization is in the process of developing its information security program that involves working with several complex organizational functions. Which of the following will BEST enable the successful implementation of this program?

A. Security governance

B. Security policy

C. Security metrics

D. Security guidelines

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 94

Topic #: 1

[All CISM Questions]

What is the BEST reason to keep information security policies separate from procedures?

A. To keep policies from having to be changed too frequently

B. To ensure that individual documents do not contain conflicting information

C. To keep policy documents from becoming too large

D. To ensure policies receive the appropriate approvals

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 95

Topic #: 1

[All CISM Questions]

A small organization has a contract with a multinational cloud computing vendor. Which of the following would present the GREATEST concern to an information security manager if omitted from the contract?

A. Escrow of software code with conditions for code release

B. Right of the subscriber to conduct onsite audits of the vendor

C. Authority of the subscriber to approve access to its data

D. Commingling of subscribers' data on the same physical server

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 96

Topic #: 1

[All CISM Questions]

An information security manager has identified a major security event with potential noncompliance implications. Who should be notified FIRST?

A. Internal audit

B. Public relations team

C. Senior management

D. Regulatory authorities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 97

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY purpose of establishing an information security governance framework?

A. To proactively address security objectives

B. To reduce security audit issues

C. To enhance business continuity planning

D. To minimize security risks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 98

Topic #: 1

[All CISM Questions]

An organization is leveraging tablets to replace desktop computers shared by shift-based staff. These tablets contain critical business data and are inherently at increased risk of theft. Which of the following will BEST help to mitigate this risk?

A. Implement remote wipe capability.

B. Create an acceptable use policy.

C. Conduct a mobile device risk assessment.

D. Deploy mobile device management (MDM).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 99

Topic #: 1

[All CISM Questions]

When scoping a risk assessment, assets need to be classified by:

A. sensitivity and criticality.

B. likelihood and impact.

C. threats and opportunities.

D. redundancy and recoverability.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 100

Topic #: 1

[All CISM Questions]

Which of the following would BEST enable effective decision-making?

A. Annualized loss estimates determined from past security events

B. A universally applied list of generic threats, impacts, and vulnerabilities

C. A consistent process to analyze new and historical information risk

D. Formalized acceptance of risk analysis by business management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 101

Topic #: 1

[All CISM Questions]

Which of the following has the GREATEST impact on efforts to improve an organization's security posture?

A. Well-documented security policies and procedures

B. Supportive tone at the top regarding security

C. Regular reporting to senior management

D. Automation of security controls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 102

Topic #: 1

[All CISM Questions]

Which of the following is the BEST strategy to implement an effective operational security posture?

A. Increased security awareness

B. Defense in depth

C. Threat management

D. Vulnerability management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 103

Topic #: 1

[All CISM Questions]

In a cloud technology environment, which of the following would pose the GREATEST challenge to the investigation of security incidents?

A. Non-standard event logs

B. Access to the hardware

C. Data encryption

D. Compressed customer data

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 104

Topic #: 1

[All CISM Questions]

The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity planning process is to:

A. obtain the support of executive management.

B. document the disaster recovery process.

C. map the business process to supporting IT and other corporate resources.

D. identify critical processes and the degree of reliance on support services.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 105

Topic #: 1

[All CISM Questions]

Which of the following is MOST important when selecting an information security metric?

A. Ensuring the metric is repeatable

B. Aligning the metric to the IT strategy

C. Defining the metric in qualitative terms

D. Defining the metric in quantitative terms

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 106

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way for an information security manager to justify ongoing annual maintenance fees associated with an intrusion prevention system (IPS)?

A. Establish and present appropriate metrics that track performance.

B. Perform industry research annually and document the overall ranking of the IPS.

C. Perform a penetration test to demonstrate the ability to protect.

D. Provide yearly competitive pricing to illustrate the value of the IPS.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 107

Topic #: 1

[All CISM Questions]

An organization wants to enable digital forensics for a business-critical application. Which of the following will BEST help to support this objective?

A. Install biometric access control.

B. Develop an incident response plan.

C. Define data retention criteria.

D. Enable activity logging.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 108

Topic #: 1

[All CISM Questions]

An employee clicked on a link in a phishing email, triggering a ransomware attack. Which of the following should be the information security manager's FIRST step?

A. Notify internal legal counsel.

B. Isolate the impacted endpoints.

C. Wipe the affected system.

D. Notify senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 109
Topic #: 1
[All CISM Questions]

A recent audit found that an organization's new user accounts are not set up uniformly. Which of the following is MOST important for the information security manager to review?

A. Security policies

B. Automated controls

C. Guidelines

D. Standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 110

Topic #: 1

[All CISM Questions]

Which of the following metrics is the BEST measure of the effectiveness of an information security program?

A. Reduction in the amount of risk exposure in an organization

B. Reduction in the number of threats to an organization

C. Reduction in the cost of risk remediation for an organization

D. Reduction in the number of vulnerabilities in an organization

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 111

Topic #: 1

[All CISM Questions]

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

A. Update the risk assessment framework.

B. Monitor the effectiveness of controls.

C. Review the risk probability and impact.

D. Review the inherent risk level.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 112

Topic #: 1

[All CISM Questions]

The BEST way to avoid session hijacking is to use:

A. strong password controls.

B. a firewall.

C. a reverse lookup.

D. a secure protocol.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 113

Topic #: 1

[All CISM Questions]

A critical server for a hospital has been encrypted by ransomware. The hospital is unable to function effectively without this server. Which of the following would MOST effectively allow the hospital to avoid paying the ransom?

A. A continual server replication process

B. Employee training on ransomware

C. A properly tested offline backup system

D. A properly configured firewall

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 114

Topic #: 1

[All CISM Questions]

Which of the following functions is MOST critical when initiating the removal of system access for terminated employees?

A. Help desk

B. Legal

C. Information security

D. Human resources (HR)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 115

Topic #: 1

[All CISM Questions]

The authorization to transfer the handling of an internal security incident to a third-party support provider is PRIMARILY defined by the:

A. escalation procedures.

B. information security manager.

C. chain of custody.

D. disaster recovery plan (DRP).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 116

Topic #: 1

[All CISM Questions]

What is the PRIMARY objective of performing a vulnerability assessment following a business system update?

A. Improve the change control process.

B. Update the threat landscape.

C. Determine operational losses.

D. Review the effectiveness of controls.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 117

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager perform FIRST when an organization's residual risk has increased?

A. Implement security measures to reduce the risk.

B. Assess the business impact.

C. Transfer the risk to third parties.

D. Communicate the information to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 118

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY reason for an information security manager to present the business case for an information security initiative to senior management?

A. To aid management in the decision-making process for purchasing the solution

B. To represent stakeholders who will benefit from enhancements in information security

C. To provide management with the status of the information security program

D. To demonstrate to management the due diligence involved with selecting the solution

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 119

Topic #: 1

[All CISM Questions]

During a security assessment, an information security manager finds a number of security patches were not installed on a server hosting a critical business application. The application owner did not approve the patch installation to avoid interrupting the application. Which of the following should be the information security manager's FIRST course of action?

A. Report the risk to the information security steering committee.

B. Determine mitigation options with IT management.

C. Communicate the potential impact to the application owner.

D. Escalate the risk to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 120

Topic #: 1

[All CISM Questions]

Which of the following BEST indicates an effective vulnerability management program?

A. Security incidents are reported in a timely manner.

B. Threats are identified accurately.

C. Controls are managed proactively.

D. Risks are managed within acceptable limits.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 121

Topic #: 1

[All CISM Questions]

An organization has experienced multiple instances of privileged users misusing their access. Which of the following processes would be MOST helpful in identifying such violations?

A. Policy exception review

B. Review of access controls

C. Security assessment

D. Log review

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 122

Topic #: 1

[All CISM Questions]

An information security manager discovers that the organization's new information security policy is not being followed across all departments. Which of the following should be of GREATEST concern to the information security manager?

A. Business unit management has not emphasized the importance of the new policy.

B. Different communication methods may be required for each business unit.

C. The wording of the policy is not tailored to the audience.

D. The corresponding controls are viewed as prohibitive to business operations.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 123

Topic #: 1

[All CISM Questions]

Which of the following is the BEST defense against a brute force attack?

A. Intruder detection lockout

B. Time-of-day restrictions

C. Discretionary access control

D. Mandatory access control

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 124

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important reason to involve external forensics experts in evidence collection when responding to a major security breach?

A. To provide the response team with expert training on evidence handling

B. To ensure evidence is handled by qualified resources

C. To prevent evidence from being disclosed to any internal staff members

D. To validate the incident response process

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 125

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST benefit of integrating information security program requirements into vendor management?

A. The ability to meet industry compliance requirements

B. The ability to define service level agreements (SLAs)

C. The ability to reduce risk in the supply chain

D. The ability to improve vendor performance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 126

Topic #: 1

[All CISM Questions]

Who should determine data access requirements for an application hosted at an organization's data center?

A. Information security manager

B. Business owner

C. Data custodian

D. Systems administrator

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 127

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important objective of testing a security incident response plan?

A. Ensure the thoroughness of the response plan.

B. Verify the response assumptions are valid.

C. Confirm that systems are recovered in the proper order.

D. Validate the business impact analysis (BIA).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 128

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important reason for performing a cost-benefit analysis when implementing a security control?

A. To ensure that the mitigation effort does not exceed the asset value

B. To ensure that benefits are aligned with business strategies

C. To present a realistic information security budget

D. To justify information security program activities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 129

Topic #: 1

[All CISM Questions]

An information security manager wants to document requirements detailing the minimum security controls required for user workstations. Which of the following resources would be MOST appropriate for this purpose?

A. Policies

B. Standards

C. Procedures

D. Guidelines

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 130

Topic #: 1

[All CISM Questions]

Which of the following information BEST supports risk management decision making?

A. Results of a vulnerability assessment

B. Estimated savings resulting from reduced risk exposure

C. Average cost of risk events

D. Quantification of threats through threat modeling

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 131

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to do after a security incident has been verified?

A. Notify the appropriate law enforcement authorities of the incident.

B. Follow the escalation process to inform key stakeholders.

C. Prevent the incident from creating further damage to the organization.

D. Contact forensic investigators to determine the root cause.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 132

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY driver for selecting and implementing appropriate controls to address the risk associated with weak user passwords?

A. The organization's risk tolerance

B. The organization's culture

C. The cost of risk mitigation controls

D. Direction from senior management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 133

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to consider when determining the effectiveness of the information security governance program?

A. Key performance indicators (KPIs)

B. Maturity models

C. Risk tolerance levels

D. Key risk indicators (KRIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 134

Topic #: 1

[All CISM Questions]

The business advantage of implementing authentication tokens is that they:

A. provide nonrepudiation.

B. reduce overall cost.

C. reduce administrative workload.

D. improve access security.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 135

Topic #: 1

[All CISM Questions]

In an organization that has several independent security tools including intrusion detection systems (IDSs) and firewalls, which of the following is the BEST way to ensure timely detection of incidents?

A. Implement a log aggregation and correlation solution.

B. Ensure that the incident response plan is endorsed by senior management.

C. Ensure staff are cross trained to manage all security tools.

D. Outsource the management of security tools to a service provider.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 136

Topic #: 1

[All CISM Questions]

Which of the following is the MAIN objective of a risk management program?

A. Reduce corporate liability for information security incidents.

B. Reduce risk to the level of the organization's risk appetite

C. Reduce risk to the maximum extent possible

D. Reduce costs associated with incident response.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 137

Topic #: 1

[All CISM Questions]

An information security manager was informed that a planned penetration test could potentially disrupt some services. Which of the following should be the FIRST course of action?

A. Estimate the impact and inform the business owner.

B. Accept the risk and document it in the risk register.

C. Ensure the service owner is available during the penetration test.

D. Reschedule the activity during an approved maintenance window.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 138

Topic #: 1

[All CISM Questions]

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

A. support multiple authentication mechanisms.

B. strengthen user passwords.

C. increase efficiency of access management.

D. increase the security of related applications.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 139

Topic #: 1

[All CISM Questions]

Which of the following is BEST determined by using technical metrics?

A. Whether controls are operating effectively

B. How well security risk is being managed

C. Whether security resources are adequately allocated

D. How well the security strategy is aligned with organizational objectives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 140

Topic #: 1

[All CISM Questions]

The use of a business case to obtain funding for an information security investment is MOST effective when the business case:

A. relates the investment to the organization's strategic plan.

B. realigns information security objectives to organizational strategy.

C. articulates management's intent and information security directives in clear language.

D. translates information security policies and standards into business requirements.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 141

Topic #: 1

[All CISM Questions]

The MOST important objective of security awareness training for business staff is to:

A. understand intrusion methods.

B. reduce negative audit findings.

C. increase compliance.

D. modify behavior.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 142

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY responsibility of an information security steering committee?

A. Setting up password expiration procedures

B. Drafting security policies

C. Prioritizing security initiatives

D. Reviewing firewall rules

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 143

Topic #: 1

[All CISM Questions]

During a post-incident review, the sequence and correlation of actions must be analyzed PRIMARILY based on:

A. a consolidated event timeline.

B. logs from systems involved.

C. interviews with personnel.

D. documents created during the incident.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 144

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important element in the evaluation of inherent security risks?

A. Impact to the organization

B. Control effectiveness

C. Residual risk

D. Cost of countermeasures

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 145

Topic #: 1

[All CISM Questions]

Recovery time objectives (RTOs) are an output of which of the following?

A. Business continuity plan (BCP)

B. Business impact analysis (BIA)

C. Service level agreement (SLA)

D. Disaster recovery plan (DRP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 146

Topic #: 1

[All CISM Questions]

Which of the following is the MOST relevant information to include in an information security risk report to facilitate senior management's understanding of impact to the organization?

A. Detailed assessment of the security risk profile

B. Risks inherent in new security technologies

C. Findings from recent penetration testing

D. Status of identified key security risks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 147

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to include in a contract with a critical service provider to help ensure alignment with the organization's information security program?

A. Escalation paths

B. Termination language

C. Key performance indicators (KPIs)

D. Right-to-audit clause

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 148

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to determine if a recent investment in access control software was successful?

A. Senior management acceptance of the access control software

B. A comparison of security incidents before and after software installation

C. A business impact analysis (BIA) of the systems protected by the software

D. A review of the number of key risk indicators (KRIs) implemented for the software

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 149

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to mitigate the risk of confidential data leakage to unauthorized stakeholders?

A. Create a data classification policy.

B. Implement role-based access controls.

C. Require the use of login credentials and passwords.

D. Conduct information security awareness training.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 150

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when reporting the effectiveness of an information security program to key business stakeholders?

A. Linking security metrics to the business impact analysis (BIA)

B. Demonstrating a decrease in information security incidents

C. Demonstrating cost savings of each control

D. Linking security metrics to business objectives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 151

Topic #: 1

[All CISM Questions]

The PRIMARY purpose of establishing an information security governance framework should be to:

A. establish the business case for strategic integration of information security in organizational efforts.

B. document and communicate how the information security program functions within the organization.

C. align information security strategy and investments to support organizational activities.

D. align corporate governance, activities, and investments to information security goals.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 152

Topic #: 1

[All CISM Questions]

Senior management is concerned that the incident response team took unapproved actions during incident response that put business objectives at risk. Which of the following is the BEST way for the information security manager to respond to this situation?

A. Update roles and responsibilities of the incident response team.

B. Train the incident response team on escalation procedures.

C. Implement a monitoring solution for incident response activities.

D. Validate that the information security strategy maps to corporate objectives.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 153

Topic #: 1

[All CISM Questions]

An incident response team has determined there is a need to isolate a system that is communicating with a known malicious host on the Internet. Which of the following stakeholders should be contacted FIRST?

A. The business owner

B. Key customers

C. Executive management

D. System administrator

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 154

Topic #: 1

[All CISM Questions]

Which of the following external entities would provide the BEST guidance to an organization facing advanced attacks?

A. Incident response experts from highly regarded peer organizations

B. Open-source reconnaissance

C. Recognized threat intelligence communities

D. Disaster recovery consultants widely endorsed in industry forums

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 155

Topic #: 1

[All CISM Questions]

Which of the following should be an information security manager's MOST important criterion for determining when to review the incident response plan?

A. When recovery time objectives (RTOs) are not met

B. When missing information impacts recovery from an incident

C. Before an internal audit of the incident response process

D. At intervals indicated by industry best practice

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 156

Topic #: 1

[All CISM Questions]

During which stage of the software development life cycle (SDLC) should application security controls FIRST be addressed?

A. Software code development

B. Configuration management

C. Requirements gathering

D. Application system design

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 157

Topic #: 1

[All CISM Questions]

Which of the following should be of MOST concern to an information security manager reviewing an organization's data classification program?

A. The classifications do not follow industry best practices.

B. Labeling is not consistent throughout the organization.

C. The program allows exceptions to be granted.

D. Data retention requirements are not defined.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 158

Topic #: 1

[All CISM Questions]

Which of the following is PRIMARILY influenced by a business impact analysis (BIA)?

A. Recovery strategy

B. Risk mitigation strategy

C. Security strategy

D. IT strategy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 159

Topic #: 1

[All CISM Questions]

The MAIN purpose of influenced by a business impact guideline for use within a large, international organization is to:

A. explain the organization's preferred practices for security.

B. ensure that all business units have the same strategic security goals.

C. ensure that all business units implement identical security procedures.

D. provide evidence for auditors that security practices are adequate.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 160

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST course of action upon discovering an organization with budget constraints lacks several important security capabilities?

A. Suggest the deployment of open-source security tools to mitigate identified risks.

B. Establish a business case to demonstrate return on investment (ROI) of a security tool.

C. Recommend that the organization avoid the most severe risks.

D. Review the most recent audit report and request funding to address the most serious finding.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 161

Topic #: 1

[All CISM Questions]

What is the FIRST line of defense against criminal insider activities?

A. Signing security agreements by critical personnel

B. Stringent and enforced access controls

C. Validating the integrity of personnel

D. Monitoring employee activities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 162

Topic #: 1

[All CISM Questions]

The BEST way to report to the board on the effectiveness of the information security program is to present:

A. a summary of the most recent audit findings.

B. a report of cost savings from process improvements.

C. peer-group industry benchmarks.

D. a dashboard illustrating key performance metrics.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 163

Topic #: 1

[All CISM Questions]

An organization's outsourced firewall was poorly configured and allowed unauthorized access that resulted in downtime of 48 hours. Which of the following should be the information security manager's NEXT course of action?

A. Reconfigure the firewall in accordance with best practices.

B. Obtain supporting evidence that the problem has been corrected.

C. Seek damages from the service provider.

D. Revisit the contract and improve accountability of the service provider.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 164

Topic #: 1

[All CISM Questions]

Which is the MOST important requirement when establishing a process for responding to zero-day vulnerabilities?

A. The IT team updates antivirus signatures on user systems.

B. The IT team implements an emergency patch deployment process.

C. Business users stop using the impacted application until a patch is released.

D. The information security team implements recommended workarounds.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 165

Topic #: 1

[All CISM Questions]

An information security manager has determined that the mean time to prioritize information security incidents has increased to an unacceptable level. Which of the following processes would BEST enable the information security manager to address this concern?

A. Incident classification

B. Incident response

C. Forensic analysis

D. Vulnerability assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 166

Topic #: 1

[All CISM Questions]

An information security manager discovers that newly hired privileged users are not taking necessary steps to protect critical information at their workstations. Which of the following is the BEST way to address this situation?

A. Publish an acceptable use policy and require signed acknowledgment.

B. Turn on logging and record user activity.

C. Communicate the responsibility and provide appropriate training.

D. Implement a data loss prevention (DLP) solution.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 167

Topic #: 1

[All CISM Questions]

Which of the following should be the MOST important consideration when prioritizing risk remediation?

A. Evaluation of risk

B. Duration of exposure

C. Comparison to risk appetite

D. Impact of compliance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 168

Topic #: 1

[All CISM Questions]

To set security expectations across the enterprise, it is MOST important for the information security policy to be regularly reviewed and endorsed by:

A. security administrators.

B. senior management.

C. the chief information security officer (CISO).

D. the IT steering committee.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 169

Topic #: 1

[All CISM Questions]

Senior management wants to provide mobile devices to its sales force. Which of the following should the information security manager do FIRST to support this objective?

A. Develop an acceptable use policy

B. Conduct a vulnerability assessment on the devices

C. Assess risks introduced by the technology

D. Research mobile device management (MDM) solutions

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 170

Topic #: 1

[All CISM Questions]

An information security manager needs to ensure security testing is conducted on a new system. Which of the following would provide the HIGHEST level of assurance?

A. The vendor provides the results of a penetration test and code review.

B. An independent party is directly engaged to conduct testing.

C. The internal audit team is enlisted to run a vulnerability assessment against the system.

D. The security team conducts a self-assessment against a recognized industry framework.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 171

Topic #: 1

[All CISM Questions]

An organization performed a risk analysis and found a large number of assets with low-impact vulnerabilities. The NEXT action of the information security manager should be to:

A. transfer the risk to a third party.

B. determine appropriate countermeasures.

C. report to management.

D. quantify the aggregated risk.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 172

Topic #: 1

[All CISM Questions]

Organization A offers e-commerce services and uses secure transport protocol to protect Internet communication. To confirm communication with Organization A, which of the following would be the BEST for a client to verify?

A. The URL of the e-commerce server

B. The certificate of the e-commerce server

C. The IP address of the e-commerce server

D. The browser's indication of SSL use

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 173

Topic #: 1

[All CISM Questions]

Which of the following provides the MOST useful information for identifying security control gaps on an application server?

A. Risk assessments

B. Penetration testing

C. Threat models

D. Internal audit reports

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 174

Topic #: 1

[All CISM Questions]

Which of the following components of an information security risk assessment is MOST valuable to senior management?

A. Residual risk

B. Return on investment (ROI)

C. Mitigation actions

D. Threat profile

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 175

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY benefit of implementing a maturity model for information security management?

A. Gaps between current and desirable levels will be addressed.

B. Information security management costs will be optimized.

C. Information security strategy will be in line with industry best practice.

D. Staff awareness of information security compliance will be promoted.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 176

Topic #: 1

[All CISM Questions]

An information security manager notes that security incidents are not being appropriately escalated by the help desk after tickets are logged. Which of the following is the BEST automated control to resolve this issue?

A. Integrating automated service level agreement (SLA) reporting into the help desk ticketing system

B. Changing the default setting for all security incidents to the highest priority

C. Integrating incident response workflow into the help desk ticketing system

D. Implementing automated vulnerability scanning in the help desk workflow

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 177

Topic #: 1

[All CISM Questions]

An information security manager's PRIMARY objective for presenting key risks to the board of directors is to:

A. ensure appropriate information security governance.

B. quantify reputational risks.

C. meet information security compliance requirements.

D. re-evaluate the risk appetite.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 178

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY consideration when implementing a data loss prevention (DLP) solution?

A. Data ownership

B. Data storage capabilities

C. Data classification

D. Selection of tools

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 179

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important function of an information security steering committee?

A. Evaluating the effectiveness of information security controls on a periodic basis

B. Defining the objectives of the information security framework

C. Conducting regular independent reviews of the state of security in the business

D. Approving security awareness content prior to publication

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 180

Topic #: 1

[All CISM Questions]

When determining an acceptable risk level, which of the following is the MOST important consideration?

A. Vulnerability scores

B. System criticalities

C. Risk matrices

D. Threat profiles

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 181

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to include when reporting information security risk to executive leadership?

A. Key performance objectives and budget trends

B. Security awareness training participation and residual risk exposures

C. Risk analysis results and key risk indicators (KRIs)

D. Information security risk management plans and control compliance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 182

Topic #: 1

[All CISM Questions]

During which of the following development phases is it MOST challenging to implement security controls?

A. Implementation phase

B. Post-implementation phase

C. Design phase

D. Development phase

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 183

Topic #: 1

[All CISM Questions]

An employee is found to be using an external cloud storage service to share corporate information with a third-party consultant, which is against company policy. Which of the following should be the information security manager's FIRST course of action?

A. Block access to the cloud storage service

B. Determine the classification level of the information

C. Seek business justification from the employee

D. Inform higher management of a security breach

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 184

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective method of determining security priorities?

A. Vulnerability assessment

B. Gap analysis

C. Threat assessment

D. Impact analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 185

Topic #: 1

[All CISM Questions]

A measure of the effectiveness of the incident response capabilities of an organization is the:

A. number of incidents detected.

B. number of employees receiving incident response training.

C. reduction of the annual loss expectancy (ALE).

D. time to closure of incidents.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 186

Topic #: 1

[All CISM Questions]

An organization is in the process of adopting a hybrid data infrastructure, transferring all non-core applications to cloud service providers, and maintaining all core business functions in-house. The information security manager has determined a defense in depth strategy should be used. Which of the following BEST describes this strategy?

A. Separate security controls for applications, platforms, programs, and endpoints

B. Multi-factor login requirements for cloud service applications, timeouts, and complex passwords

C. Deployment of nested firewalls within the infrastructure

D. Strict enforcement of role-based access control (RBAC)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 187

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST approach when selecting cost-effective controls needed to meet business objectives?

A. Conduct a gap analysis.

B. Focus on preventive controls.

C. Align with industry best practice.

D. Align with the risk appetite.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 188

Topic #: 1

[All CISM Questions]

A risk was identified during a risk assessment. The business process owner has chosen to accept the risk because the cost of remediation is greater than the projected cost of a worst-case scenario. What should be the information security manager's NEXT course of action?

A. Document and schedule a date to revisit the issue.

B. Document and escalate to senior management.

C. Shut down the business application.

D. Determine a lower-cost approach to remediation.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 189

Topic #: 1

[All CISM Questions]

An organization wants to integrate information security into its human resource management processes. Which of the following should be the FIRST step?

A. Identify information security risk associated with the processes

B. Assess the business objectives of the processes

C. Evaluate the cost of information security integration

D. Benchmark the processes with best practice to identify gaps

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 190

Topic #: 1

[All CISM Questions]

The MOST effective way to continuously monitor an organization's cybersecurity posture is to evaluate its:

A. compliance with industry regulations.

B. key performance indicators (KPIs).

C. level of support from senior management.

D. timeliness in responding to attacks.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 191

Topic #: 1

[All CISM Questions]

Which of the following would provide the HIGHEST level of confidence in the integrity of data when sent from one party to another?

A. Harden the communication infrastructure.

B. Require files to be digitally signed before they are transmitted.

C. Enforce multi-factor authentication on both ends of the communication.

D. Require data to be transmitted over a secure connection.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 192

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to the successful implementation of an information security program?

A. Establishing key performance indicators (KPIs)

B. Obtaining stakeholder input

C. Understanding current and emerging technologies

D. Conducting periodic risk assessments

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 193

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to strengthen the alignment of an information security program with business strategy?

A. Establishing an information security steering committee

B. Increasing the frequency of control assessments

C. Providing organizational training on information security policies

D. Increasing budget for risk assessments

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 194

Topic #: 1

[All CISM Questions]

Which of the following is necessary to determine what would constitute a disaster for an organization?

A. Recovery strategy analysis

B. Backup strategy analysis

C. Risk analysis

D. Threat probability analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 195

Topic #: 1

[All CISM Questions]

Management has announced the acquisition of a new company. The information security manager of the parent company is concerned that conflicting access rights may cause critical information to be exposed during the integration of the two companies. To BEST address this concern, the information security manager should:

A. escalate concerns for conflicting access rights to management.

B. review access rights as the acquisition integration occurs.

C. implement consistent access control standards.

D. perform a risk assessment of the access rights.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 196

Topic #: 1

[All CISM Questions]

Which of the following metrics provides the BEST measurement of the effectiveness of a security awareness program?

A. Variance of program cost to allocated budget

B. The number of security breaches

C. Mean time between incident detection and remediation

D. The number of reported security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 197

Topic #: 1

[All CISM Questions]

The ULTIMATE responsibility for ensuring the objectives of an information security framework are being met belongs to:

A. the board of directors.

B. the information security officer.

C. the steering committee.

D. the internal audit manager.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 198

Topic #: 1

[All CISM Questions]

Which of the following is MOST likely to affect an organization's ability to respond to security incidents in a timely manner?

A. Lack of senior management buy-in

B. Inadequate detective control performance

C. Misconfiguration of security information and event management (SIEM) tool

D. Complexity of network segmentation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 199

Topic #: 1

[All CISM Questions]

After a server has been attacked, which of the following is the BEST course of action?

A. Isolate the system.

B. Initiate incident response.

C. Conduct a security audit.

D. Review vulnerability assessment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 200

Topic #: 1

[All CISM Questions]

When establishing classifications of security incidents for the development of an incident response plan, which of the following provides the MOST valuable input?

A. Business impact analysis (BIA) results

B. Recommendations from senior management

C. The business continuity plan (BCP)

D. Vulnerability assessment results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 201

Topic #: 1

[All CISM Questions]

What is the PRIMARY responsibility of the security steering committee?

A. Implement information security control.

B. Develop information security policy.

C. Set direction and monitor performance.

D. Provide information security training to employees.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 202

Topic #: 1

[All CISM Questions]

The PRIMARY objective of a risk response strategy should be:

A. threat reduction.

B. senior management buy-in.

C. appropriate control selection.

D. regulatory compliance.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 203

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST after a new cybersecurity regulation has been introduced?

A. Consult corporate legal counsel.

B. Conduct a cost-benefit analysis.

C. Update the information security policy.

D. Perform a gap analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 204

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important security feature an information security manager would need for a mobile device management (MDM) program?

A. Ability to inventory devices

B. Ability to remotely wipe devices

C. Ability to locate devices

D. Ability to push updates to devices

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 205

Topic #: 1

[All CISM Questions]

Which of the following is the MOST relevant factor when determining the appropriate escalation process in the incident response plan?

A. Significance of the affected systems

B. Number of resources allocated to respond

C. Resilience capability of the affected systems

D. Replacement cost of the affected systems

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 206

Topic #: 1

[All CISM Questions]

Management has expressed concerns to the information security manager that shadow IT may be a risk to the organization. What is the FIRST step the information security manager should take?

A. Block the end user's ability to use shadow IT

B. Update the security policy to address shadow IT

C. Determine the value of shadow IT projects

D. Determine the extent of shadow IT usage

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 207

Topic #: 1

[All CISM Questions]

The PRIMARY purpose for defining key risk indicators (KRIs) for a security program is to:

A. support investments in the security program.

B. compare security program effectiveness to benchmarks.

C. provide information needed to take action.

D. ensure mitigating controls meet specifications.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 208

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to protect the authenticity of data in transit?

A. Digital signature

B. Hash value

C. Private key

D. Public key

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 209
Topic #: 1
[All CISM Questions]

An organization shares customer information across its globally dispersed branches. Which of the following should be the GREATEST concern to information security management?

A. Conflicting data protection regulations

B. Cross-cultural differences between branches

C. Insecure wide area networks (WANs)

D. Decentralization of information security

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 210

Topic #: 1

[All CISM Questions]

An information security manager is assisting in the development of the request for proposal (RFP) for a new outsourced service. This will require the third party to have access to critical business information. The security manager should focus PRIMARILY on defining:

A. security requirements for the process being outsourced

B. risk-reporting methodologies

C. service level agreements (SLAs)

D. security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 211

Topic #: 1

[All CISM Questions]

Following a risk assessment, new countermeasures have been approved by management. Which of the following should be performed NEXT?

A. Schedule the target end date for implementation activities.

B. Develop an implementation strategy.

C. Budget the total cost of implementation activities.

D. Calculate the cost for each countermeasure.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 212

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective defense against malicious insiders compromising confidential information?

A. Regular audits of access controls

B. Strong background checks when hiring staff

C. Prompt termination procedures

D. Role-based access control

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 213

Topic #: 1

[All CISM Questions]

An information security manager is asked to provide a short presentation on the organization's current IT risk posture to the board of directors. Which of the following would be MOST effective to include in this presentation?

A. Gap analysis results

B. Risk register

C. Threat assessment results

D. Risk heat map

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 214

Topic #: 1

[All CISM Questions]

Which of the following provides the BEST assurance that a contracted third-party provider meets an organization's security requirements?

A. Continuous monitoring

B. Due diligence questionnaires

C. Right-to-audit clause in the contract

D. Performance metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 215

Topic #: 1

[All CISM Questions]

An organization's senior management is encouraging employees to use social media for promotional purposes. Which of the following should be the information security manager s FIRST step to support this strategy?

A. Incorporate social media into the security awareness program.

B. Develop a guideline on the acceptable use of social media.

C. Employ the use of a web content filtering solution.

D. Develop a business case for a data loss prevention (DLP) solution.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 216

Topic #: 1

[All CISM Questions]

In addition to executive sponsorship and business alignment, which of the following is MOST critical for information security governance?

A. Ownership of security

B. Auditability of systems

C. Allocation of training resources

D. Compliance with policies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 217

Topic #: 1

[All CISM Questions]

Which of the following is a PRIMARY responsibility of the information security governance function?

A. Administering information security awareness training

B. Advising senior management on optimal levels of risk appetite and tolerance

C. Defining security strategies to support organizational programs

D. Ensuring adequate support for solutions using emerging technologies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 218

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to the successful implementation of an information security program?

A. Key performance indicators (KPIs) are defined.

B. Adequate security resources are allocated to the program.

C. A balanced scorecard is approved by the steering committee.

D. The program is developed using global security standards.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 219

Topic #: 1

[All CISM Questions]

To address the issue that performance pressures on IT may conflict with information security controls, it is MOST important that:

A. the steering committee provides guidance and dispute resolution.

B. the security policy is changed to accommodate IT performance pressure.

C. IT policies and procedures are better aligned to security policies.

D. noncompliance issues are reported to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 220

Topic #: 1

[All CISM Questions]

Information security awareness programs are MOST effective when they are:

A. sponsored by senior management.

B. reinforced by computer-based training.

C. customized for each target audience.

D. conducted at employee orientation.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 221

Topic #: 1

[All CISM Questions]

Which of the following would BEST help an organization's ability to manage advanced persistent threats (APT)?

A. Having a skilled information security team

B. Increasing the information security budget

C. Using multiple security vendors

D. Having network detection tools in place

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 222

Topic #: 1

[All CISM Questions]

An employee has just reported the loss of a personal mobile device containing corporate information. Which of the following should the information security manager do FIRST?

A. Initiate incident response.

B. Initiate a device reset.

C. Conduct a risk assessment.

D. Disable remote access.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 223

Topic #: 1

[All CISM Questions]

An organization has fallen victim to a spear-phishing attack that compromised the multi-factor authentication code. What is the information security manager's MOST important follow-up action?

A. Communicate the threat to users.

B. Install client anti-malware solutions.

C. Implement firewall blocking of known attack signatures.

D. Implement an advanced email filtering system.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 224

Topic #: 1

[All CISM Questions]

Which of the following is MOST important for an information security manager to communicate to stakeholders when approving exceptions to the information security policy?

A. Impact on the risk profile

B. Need for compensating controls

C. Time period for review

D. Requirements for senior management reporting

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 225

Topic #: 1

[All CISM Questions]

To implement effective continuous monitoring of IT controls, an information security manager needs to FIRST ensure:

A. security alerts are centralized.

B. periodic scanning of IT systems is in place.

C. metrics are communicated to senior management.

D. information assets have been classified.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 226

Topic #: 1

[All CISM Questions]

Which of the following would provide the BEST evidence to senior management that security control performance has improved?

A. Demonstrated return on security investment

B. Review of security metrics trends

C. Results of an emerging threat analysis

D. Reduction in inherent risk

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 227
Topic #: 1
[All CISM Questions]

An information security manager has identified the organization is not in compliance with new legislation that will soon be in effect. Which of the following is MOST important to consider when determining additional controls to be implemented?

A. The information security strategy

B. The organization's risk appetite

C. The cost of noncompliance

D. The information security policy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 228

Topic #: 1

[All CISM Questions]

The PRIMARY benefit of a centralized time server is that it:

A. decreases the likelihood of an unrecoverable systems failure.

B. reduces individual time-of-day requests by client applications.

C. allows decentralized logs to be kept in synchronization.

D. is required by password synchronization programs.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 229

Topic #: 1

[All CISM Questions]

Which of the following is MOST appropriate to communicate to senior management regarding information risk?

A. Risk profile changes

B. Vulnerability scanning progress

C. Defined risk appetite

D. Emerging security technologies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 230

Topic #: 1

[All CISM Questions]

A new information security manager finds that the organization tends to use short-term solutions to address problems. Resource allocation and spending are not effectively tracked, and there is no assurance that compliance requirements are being met. What should be done FIRST to reverse this bottom-up approach to security?

A. Implement an information security awareness training program.

B. Conduct a threat analysis.

C. Establish an audit committee.

D. Create an information security steering committee.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 231

Topic #: 1

[All CISM Questions]

An information security manager has been tasked with developing materials to update the board, regulatory agencies, and the media about a security incident.
Which of the following should the information security manager do FIRST?

A. Invoke the organization's incident response plan.

B. Set up communication channels for the target audience.

C. Create a comprehensive singular communication.

D. Determine the needs and requirements of each audience.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 232

Topic #: 1

[All CISM Questions]

Which of the following is MOST appropriate to add to a dashboard for the purpose of illustrating an organization's risk level to senior management?

A. Results of risk and control testing

B. Number of reported incidents

C. Budget variance for information security

D. Risk heat map

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 233

Topic #: 1

[All CISM Questions]

When establishing escalation processes for an organization's computer security incident response team, the organization's procedures should:

A. require events to be escalated whenever possible to ensure that management is kept informed.

B. provide unrestricted communication channels to executive leadership to ensure direct access.

C. specify step-by-step escalation paths to ensure an appropriate chain of command.

D. recommend the same communication path for events to ensure consistency of communication.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 234

Topic #: 1

[All CISM Questions]

Which of the following is the MOST beneficial outcome of testing an incident response plan?

A. The response includes escalation to senior management.

B. Test plan results are documented.

C. Incident response time is improved.

D. The plan is enhanced to reflect the findings of the test.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 235

Topic #: 1

[All CISM Questions]

The PRIMARY goal of a post-incident review should be to:

A. identify policy changes to prevent a recurrence.

B. establish the cost of the incident to the business.

C. determine why the incident occurred.

D. determine how to improve the incident handling process.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 236

Topic #: 1

[All CISM Questions]

Which of the following will MOST effectively minimize the chance of inadvertent disclosure of confidential information?

A. Applying data classification rules

B. Following the principle of least privilege

C. Restricting the use of removable media

D. Enforcing penalties for security policy violations

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 237

Topic #: 1

[All CISM Questions]

Which type of control is an incident response team?

A. Detective

B. Directive

C. Corrective

D. Preventive

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 238

Topic #: 1

[All CISM Questions]

It is MOST important for an information security manager to ensure that security risk assessments are performed:

A. during a root cause analysis.

B. as part of the security business case.

C. consistently throughout the enterprise.

D. in response to the threat landscape.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 239

Topic #: 1

[All CISM Questions]

Which of the following BEST indicates the effectiveness of the vendor risk management process?

A. Increase in the percentage of vendors certified to a globally recognized security standard

B. Increase in the percentage of vendors with a completed due diligence review

C. Increase in the percentage of vendors conducting mandatory security training

D. Increase in the percentage of vendors that have reported security breaches

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 240

Topic #: 1

[All CISM Questions]

An organization has decided to store production data in a cloud environment. What should be the FIRST consideration?

A. Data transfer

B. Data classification

C. Data backup

D. Data isolation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 241

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY reason that an information security manager would contract with an external provider to perform penetration testing?

A. To obtain an independent network security certification

B. To mitigate gaps in technical skills

C. To obtain an independent view of vulnerabilities

D. To obtain the full list of system vulnerabilities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 242

Topic #: 1

[All CISM Questions]

An organization has decided to outsource its disaster recovery function. Which of the following is the MOST important consideration when drafting the service level agreement (SLA)?

A. Testing requirements

B. Authorization chain

C. Recovery time objectives (RTOs)

D. Recovery point objectives (RPOs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 243

Topic #: 1

[All CISM Questions]

What is the PRIMARY objective of implementing standard security configurations?

A. Maintain a flexible approach to mitigate potential risk to unsupported systems.

B. Minimize the operational burden of managing and monitoring unsupported systems.

C. Compare configurations between supported and unsupported systems.

D. Control vulnerabilities and reduce threats from changed configurations.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 244

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to ensure when considering exceptions to an information security policy?

A. Exceptions are approved by executive management.

B. Exceptions undergo regular review.

C. Exceptions reflect the organizational risk appetite.

D. Exceptions are based on data classification.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 245

Topic #: 1

[All CISM Questions]

An external security audit has reported multiple instances of control noncompliance. Which of the following is MOST important for the information security manager to communicate to senior management?

A. The impact of noncompliance on the organization's risk profile

B. An accountability report to initiate remediation activities

C. Control owner responses based on a root cause analysis

D. A plan for mitigating the risk due to noncompliance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 246

Topic #: 1

[All CISM Questions]

An organization's security policy is to disable access to USB storage devices on laptops and desktops. Which of the following is the STRONGEST justification for granting an exception to the policy?

A. Users accept the risk of noncompliance.

B. The benefit is greater than the potential risk.

C. USB storage devices are enabled based on user roles.

D. Access is restricted to read-only.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 247

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's FIRST priority after a high-profile system has been compromised?

A. Implement improvements to prevent recurrence.

B. Identify the malware that compromised the system.

C. Restore the compromised system.

D. Preserve incident-related data.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 248

Topic #: 1

[All CISM Questions]

Which of the following has the MOST direct impact on the usability of an organization's asset classification policy?

A. The granularity of classifications in the hierarchy

B. The support of IT management for the classification scheme

C. The frequency of updates to the organization's risk register

D. The business objectives of the organization

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 249

Topic #: 1

[All CISM Questions]

A corporate information security program is BEST positioned for success when:

A. staff is receptive to the program.

B. senior management supports the program.

C. security is thoroughly assessed in the program.

D. the program aligns with industry best practice.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 250

Topic #: 1

[All CISM Questions]

Following a significant change to the underlying code of an application, it is MOST important for the information security manager to:

A. inform senior management.

B. update the risk assessment.

C. validate the user acceptance testing (UAT).

D. modify key risk indicators (KRIs).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 251

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY responsibility of an information security steering committee composed of management representation from business units?

A. Oversee the execution of the information security strategy.

B. Perform business impact analyses (BIAs).

C. Manage the implementation of the information security plan.

D. Monitor the treatment of information security risk.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 252

Topic #: 1

[All CISM Questions]

Audit trails of changes to source code and object code are BEST tracked through:

A. use of compilers.

B. code review.

C. program library software.

D. job control statements.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 253

Topic #: 1

[All CISM Questions]

Which of the following should be determined FIRST when preparing a risk communication plan?

A. Reporting content

B. Communication channel

C. Target audience

D. Reporting frequency

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 254

Topic #: 1

[All CISM Questions]

Which of the following will protect the confidentiality of data transmitted over the Internet?

A. Message digests

B. Encrypting file system

C. Network address translation

D. IPsec protocol

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 255

Topic #: 1

[All CISM Questions]

Which of the following would MOST effectively communicate the benefits of an information security program to executive management?

A. Key performance indicators (KPIs)

B. Threat models

C. Key risk indicators (KRIs)

D. Industry benchmarks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 256

Topic #: 1

[All CISM Questions]

Which of the following processes can be used to remediate identified technical vulnerabilities?

A. Updating the business impact analysis (BIA)

B. Performing penetration testing

C. Enforcing baseline configurations

D. Conducting a risk assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 257

Topic #: 1

[All CISM Questions]

Which of the following BEST enables the detection of advanced persistent threats (APTs)?

A. Vulnerability scanning

B. Security information and event management system (SIEM)

C. Internet gateway filtering

D. Periodic reviews of intrusion prevention system (IPS)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 258

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to strengthen the security of corporate data on a personal mobile device?

A. Implementing a strong password policy

B. Using containerized software

C. Mandating use of pre-approved devices

D. Implementing multi-factor authentication

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 259

Topic #: 1

[All CISM Questions]

An organization has implemented a new security control in response to a recently discovered vulnerability. Several employees have voiced concerns that the control disrupts their ability to work. Which of the following is the information security manager's BEST course of action?

A. Evaluate compensating control options.

B. Educate users about the vulnerability.

C. Accept the vulnerability.

D. Report the control risk to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 260

Topic #: 1

[All CISM Questions]

Which of the following would be MOST helpful when determining appropriate access controls for an application?

A. Industry best practices

B. Gap analysis results

C. End-user input

D. Data criticality

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 261

Topic #: 1

[All CISM Questions]

An information security manager has become aware that a third-party provider is not in compliance with the statement of work (SOW). Which of the following is the BEST course of action?

A. Assess the extent of the issue.

B. Report the issue to legal personnel.

C. Notify senior management of the issue.

D. Initiate contract renegotiation.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 262

Topic #: 1

[All CISM Questions]

An incident response team recently encountered an unfamiliar type of cyber event. Though the team was able to resolve the issue, it took a significant amount of time to identify. What is the BEST way to help ensure similar incidents are identified more quickly in the future?

A. Establish performance metrics for the team.

B. Perform a post-incident review.

C. Perform a threat analysis.

D. Implement a SIEM solution.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 263

Topic #: 1

[All CISM Questions]

Who should an information security manager contact FIRST upon discovering that a cloud-based payment system used by the organization may be infected with malware?

A. Senior management

B. Affected customers

C. Cloud service provider

D. The incident response team

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 264

Topic #: 1

[All CISM Questions]

An organization's operations have been significantly impacted by a cyberattack resulting in data loss. Once the attack has been contained, what should the security team do NEXT?

A. Update the incident response plan.

B. Perform a root cause analysis.

C. Implement compensating controls.

D. Conduct a lessons learned exercise.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 265

Topic #: 1

[All CISM Questions]

Which of the following would BEST help to ensure an organization's security program is aligned with business objectives?

A. The organization's board of directors includes a dedicated information security advisor.

B. The security strategy is reviewed and approved by the organization's steering committee.

C. Security policies are reviewed and approved by the chief information officer (CIO)

D. Business leaders receive annual information security awareness training This question has been

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 266

Topic #: 1

[All CISM Questions]

When defining and communicating roles and responsibilities between an organization and cloud service provider, which of the following situations would present the GREATEST risk to the organization's ability to ensure information risk is managed appropriately?

A. The service agreement uses a custom-developed RACI instead of an industry standard RACI to document responsibilities

B. The organization believes the provider accepted responsibility for issues affecting security that the provider did not accept

C. The organization and provider identified multiple information security responsibilities that neither party was planning to provide

D. The service agreement results in unnecessary duplication of effort because shared responsibilities have not been clearly defined

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 267

Topic #: 1

[All CISM Questions]

An IT department plans to migrate an application to the public cloud. Which of the following is the information security manager's MOST important action in support of this initiative?

A. Review cloud provider independent assessment reports.

B. Provide cloud security requirements

C. Evaluate service level agreements (SLAs)

D. Calculate security implementation costs

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 268

Topic #: 1

[All CISM Questions]

An executive's personal mobile device used for business purposes is reported lost. The information security manager should respond based on:

A. the acceptable use policy.

B. asset management guidelines.

C. the business impact analysis (BIA).

D. incident classification.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 269

Topic #: 1

[All CISM Questions]

What is the BEST approach for the information security manager to reduce the impact on a security program due to turnover within the security staff?

A. Recruit certified staff

B. Revise the information security program

C. Document security procedures

D. Ensure everyone is trained in their roles

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 270

Topic #: 1

[All CISM Questions]

Which of the following roles is BEST suited to validate user access requirements during an annual user access review?

A. Access manager

B. System administrator

C. Business owner

D. IT director

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 271

Topic #: 1

[All CISM Questions]

For an organization that is experiencing outages due to malicious code, which of the following is the BEST index of the effectiveness of countermeasures?

A. Number of virus infections detected

B. Average recovery time per incident

C. Amount of infection-related downtime

D. Number of downtime-related help desk calls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 272

Topic #: 1

[All CISM Questions]

Which of the following should be the MOST important consideration when reviewing an information security strategy?

A. Changes to the security budget

B. New business initiatives

C. Internal audit findings

D. Recent security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 273

Topic #: 1

[All CISM Questions]

Human resources (HR) is evaluating potential Software as a Service (SaaS) cloud services. Which of the following should the information security manager do FIRST to support this effort?

A. Perform a cost-benefit analysis of using cloud services

B. Conduct a security audit on the cloud service providers

C. Review the cloud service providers' control reports

D. Perform a risk assessment of adopting cloud services

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 274

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to evaluate the impact of threat events on an organization's IT operations?

A. Risk assessment

B. Penetration testing

C. Scenario analysis

D. Controls review

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 275

Topic #: 1

[All CISM Questions]

Which of the following BEST demonstrates that an anti-phishing campaign is effective?

A. Improved staff attendance in awareness sessions

B. Decreased number of incidents that have occurred

C. Decreased number of phishing emails received

D. Improved feedback on the anti-phishing campaign

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 276

Topic #: 1

[All CISM Questions]

The GREATEST benefit resulting from well-documented information security procedures is that they:

A. facilitate security training of new staff.

B. ensure that security policies are consistently applied.

C. provide a basis for auditing security practices.

D. ensure processes can be followed by temporary staff.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 277

Topic #: 1

[All CISM Questions]

Which of the following is the MOST reliable way to ensure network security incidents are identified as soon as possible?

A. Install stateful inspection firewalls.

B. Conduct workshops and training sessions with end users.

C. Collect and correlate IT infrastructure event logs.

D. Train help desk staff to identify and prioritize security incidents.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 278

Topic #: 1

[All CISM Questions]

Which of the following would BEST help to ensure compliance with an organization's information security requirements by an IT service provider?

A. Requiring an external security audit of the IT service provider

B. Defining the business recovery plan with the IT service provider

C. Defining information security requirements with internal IT

D. Requiring regular reporting from the IT service provider

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 279

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to include in an information security status report to senior management?

A. Review of information security policies

B. List of recent security events

C. Key risk indicators (KRIs)

D. Information security budget requests

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 280

Topic #: 1

[All CISM Questions]

Which of the following MOST effectively allows for disaster recovery testing without interrupting business operations?

A. Structured walk-through

B. Simulation testing

C. Parallel testing

D. Full interruption testing

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 281

Topic #: 1

[All CISM Questions]

The PRIMARY goal of the eradication phase in an incident response process is to:

A. provide effective triage and containment of the incident.

B. remove the threat and restore affected systems.

C. maintain a strict chain of custody.

D. obtain forensic evidence from the affected system.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 282

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to ensuring that incident management plans are executed effectively?

A. Management support and approval has been obtained.

B. An incident response maturity assessment has been conducted.

C. A reputable managed security services provider has been engaged.

D. The incident response team has the appropriate training.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 283

Topic #: 1

[All CISM Questions]

To inform a risk treatment decision, which of the following should the information security manager compare with the organization's risk appetite?

A. Gap analysis results

B. Level of risk treatment

C. Configuration parameters

D. Level of residual risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 284

Topic #: 1

[All CISM Questions]

Which of the following would be the MOST effective countermeasure against malicious programming that rounds down transaction amounts and transfers them to the perpetrator's account?

A. Set up an agent to run a virus-scanning program across platforms.

B. Ensure that proper controls exist for code review and release management.

C. Implement controls for continuous monitoring of middleware transactions.

D. Apply the latest patch programs to the production operating systems.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 285

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY responsibility of an information security governance committee?

A. Reviewing the information security risk register

B. Approving changes to the information security strategy

C. Discussing upcoming information security projects

D. Reviewing monthly information security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 286

Topic #: 1

[All CISM Questions]

The MOST important information for influencing management's support of information security is:

A. a report of a successful attack on a competitor.

B. a demonstration of alignment with the business strategy.

C. an identification of the overall threat landscape.

D. an identification of organizational risks.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 287

Topic #: 1

[All CISM Questions]

What should be an information security manager's MOST important consideration when reviewing a proposed upgrade to a business unit's production database?

A. Ensuring the application inventory is updated

B. Ensuring residual risk is within appetite

C. Ensuring a cost-benefit analysis is completed

D. Ensuring senior management is aware of associated risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 288

Topic #: 1

[All CISM Questions]

Prior to implementing a bring your own device (BYOD) program, it is MOST important to:

A. review currently utilized applications.

B. survey employees for requested applications.

C. select mobile device management (MDM) software.

D. develop an acceptable use policy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 289

Topic #: 1

[All CISM Questions]

When developing an incident escalation process, the BEST approach is to classify incidents based on:

A. their root causes.

B. information assets affected.

C. recovery point objectives (RPOs).

D. estimated time to recover.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 290

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY objective of defining a severity hierarchy for security incidents?

A. To streamline the risk analysis process

B. To facilitate the classification of an organization's IT assets

C. To prioritize available incident response resources

D. To facilitate root cause analysis of incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 291

Topic #: 1

[All CISM Questions]

For an enterprise implementing a bring your own device (BYOD) program, which of the following would provide the BEST security of corporate data residing on unsecured mobile devices?

A. Device certification process

B. Acceptable use policy

C. Containerization solution

D. Data loss prevention (DLP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 292

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY driver for delaying the delivery of an information security awareness program?

A. Change in senior management

B. High employee turnover

C. Employee acceptance

D. Risk appetite

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 293

Topic #: 1

[All CISM Questions]

An organization is developing a disaster recovery strategy and needs to identify each application's criticality so that the recovery sequence can be established. Which of the following is the BEST course of action?

A. Restore the applications with the shortest recovery times first

B. Document the data flow and review the dependencies

C. Perform a business impact analysis (BIA) on each application

D. Identify which applications contribute the most cash flow

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 294

Topic #: 1

[All CISM Questions]

An organization's IT department needs to implement security patches. Recent reports indicate these patches could result in stability issues. Which of the following is the information security manager's BEST recommendation?

A. Research alternative software solutions

B. Evaluate the patches in a test environment

C. Increase monitoring after patch implementation

D. Research compensating security controls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 295

Topic #: 1

[All CISM Questions]

An organization has established a bring your own device (BYOD) program. Which of the following is the MOST important security consideration when allowing employees to use personal devices for corporate applications remotely?

A. Mandatory controls for maintaining security policy

B. Mobile operating systems support

C. Security awareness training

D. Secure application development

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 296

Topic #: 1

[All CISM Questions]

What is the BEST way for an information security manager to ensure critical assets are prioritized in a new information security program?

A. Update operating procedures to include new requirements.

B. Conduct security awareness training.

C. Conduct an inventory of information assets.

D. Backup information assets and store them offsite.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 297

Topic #: 1

[All CISM Questions]

Which of the following would provide the MOST useful information when prioritizing controls to be added to a system?

A. The risk register

B. Balanced scorecard

C. Compliance requirements

D. Baseline to industry standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 298

Topic #: 1

[All CISM Questions]

An organization has recently acquired a smaller company located in a different geographic region. Which of the following is the BEST approach for addressing conflicts between the parent organization's security standards and local regulations affecting the acquired company?

A. Adopt the standards of the newly acquired company

B. Give precedence to the parent organization's standards

C. Create a local version of the parent organization's standards

D. Create a global version of the local regulations

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 299

Topic #: 1

[All CISM Questions]

A new regulatory requirement affecting an organization's information security program is released. Which of the following should be the information security manager's FIRST course of action?

A. Conduct benchmarking

B. Perform a gap analysis

C. Notify the legal department

D. Determine the disruption to the business

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 300

Topic #: 1

[All CISM Questions]

An organization wants to ensure its confidential data is isolated in a multi-tenanted environment at a well-known cloud service provider. Which of the following is the BEST way to ensure the data is adequately protected?

A. Verify the provider follows a cloud service framework standard.

B. Review the provider's information security policies and procedures.

C. Obtain documentation of the encryption management practices.

D. Ensure an audit of the provider is conducted to identify control gaps.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 301

Topic #: 1

[All CISM Questions]

The BEST indication of a change in risk that may negatively impact an organization is an increase in the number of:

A. security incidents reported by staff to the information security team.

B. malware infections detected by the organization's anti-virus software.

C. alerts triggered by the security information and event management (SIEM) solution.

D. events logged by the intrusion detection system (IDS).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 302

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to consider when determining the criticality and sensitivity of an information asset?

A. Results of business continuity testing

B. Number of threats that can impact the asset

C. Investment required to protect the asset

D. Business functions supported by the asset

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 303

Topic #: 1

[All CISM Questions]

To prevent ransomware attacks, it is MOST important to ensure:

A. adequate backup and restoration processes are in place.

B. regular security awareness training is conducted.

C. the latest security appliances are installed.

D. updated firewall software is installed.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 304

Topic #: 1

[All CISM Questions]

A security policy exception is leading to an unexpected increase in the number of alerts about suspicious Internet traffic on an organization's network. Which of the following is the BEST course of action?

A. Remove the rules that trigger the increased number of alerts.

B. Present a risk analysis with recommendations to senior management.

C. Update the risk register so that senior management is kept informed.

D. Evaluate and update the enterprise network security architecture.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 305

Topic #: 1

[All CISM Questions]

The MAIN purpose of documenting information security guidelines for use within a large, international organization is to:

A. explain the organization's preferred practices for security.

B. ensure that all business units have the same strategic security goals.

C. ensure that all business units implement identical security procedures.

D. provide evidence for auditors that security practices are adequate.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 306

Topic #: 1

[All CISM Questions]

Senior management has launched an enterprise-wide initiative to streamline internal processes to reduce costs, including security processes. What should the information security manager rely on MOST to allocate resources efficiently?

A. Capability maturity assessment

B. Risk classification

C. Return on investment (ROI)

D. Internal audit reports

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 307

Topic #: 1

[All CISM Questions]

Which of the following would be of GREATEST assistance in determining whether to accept residual risk of a critical security system?

A. Maximum tolerable outage (MTO)

B. Recovery time objective (RTO)

C. Available annual budget

D. Cost-benefit analysis of mitigating controls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 308

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST to address complaints that a newly implemented security control has slowed business operations?

A. Conduct user awareness training.

B. Remove the control and identify alternatives.

C. Discuss the issue with senior management for direction.

D. Validate whether the control is operating as intended.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 309

Topic #: 1

[All CISM Questions]

An information security manager is preparing incident response plans for an organization that processes personal and financial information. Which of the following is the MOST important consideration?

A. Aligning with an established industry framework

B. Determining budgetary constraints

C. Identifying regulatory requirements

D. Aligning with enterprise architecture (EA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 310

Topic #: 1

[All CISM Questions]

An information security manager has identified that security risks are not being treated in a timely manner. Which of the following is the BEST way to address this situation?

A. Assign a risk owner to each risk.

B. Create mitigating controls to manage the risks.

C. Provide regular updates about the current state of the risks.

D. Re-perform risk analysis at regular intervals.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 311

Topic #: 1

[All CISM Questions]

Which of the following would be MOST useful in determining how an organization will be affected by a new regulatory requirement for cloud services?

A. Data loss protection plan

B. Risk assessment

C. Information asset inventory

D. Data classification policy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 312

Topic #: 1

[All CISM Questions]

Which of the following provides the BEST evidence that a newly implemented security awareness program has been effective?

A. There have been no reported successful phishing attempts since the training started.

B. Employees from each department have completed the required training.

C. There has been an increase in the number of phishing attempts reported.

D. Senior management supports funding for ongoing awareness training.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 313

Topic #: 1

[All CISM Questions]

An organization is considering the deployment of encryption software and systems organization-wide. The MOST important consideration should be whether:

A. a classification policy has been developed to incorporate the need for encryption

B. the business strategy includes exceptions to the encryption standard

C. data can be recovered if the encryption keys are misplaced

D. the implementation supports the business strategy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 314

Topic #: 1

[All CISM Questions]

From an information security perspective, legal issues associated with a transborder flow of technology-related items are MOST often related to:

A. website transactions and taxation

B. encryption tools and personal data.

C. lack of competition and free trade.

D. software patches and corporate data.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 315

Topic #: 1

[All CISM Questions]

Recovery time objectives (RTOs) are BEST determined by:

A. database administrators (DBAs).

B. business managers.

C. executive management.

D. business continuity officers.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 316

Topic #: 1

[All CISM Questions]

Embedding security responsibilities into job descriptions is important PRIMARILY because it:

A. simplifies development of the security awareness program

B. aligns security to the human resources (HR) function

C. strengthens employee accountability

D. supports access management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 317

Topic #: 1

[All CISM Questions]

An information security manager finds a legacy application has no defined data owner. Of the following, who would be MOST helpful in identifying the appropriate data owner?

A. The individual responsible for providing support for the application

B. The individual who manages the process supported by the application

C. The individual who manages users of the application

D. The individual who has the most privileges within the application

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 318

Topic #: 1

[All CISM Questions]

An online trading company discovers that a network attack has penetrated the firewall. What should be the information security manager's FIRST response?

A. Evaluate the impact to the business.

B. Examine firewall logs to identify the attacker.

C. Notify the regulatory agency of the incident.

D. Implement mitigating controls.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 319

Topic #: 1

[All CISM Questions]

Which of the following is the BEST method for determining whether a firewall has been configured to provide a comprehensive perimeter defense?

A. A port scan of the firewall from an internal source

B. A simulated denial of service (DoS) attack against the firewall

C. A validation of the current firewall rule set

D. A ping test from an external source

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 320

Topic #: 1

[All CISM Questions]

To ensure that a new application complies with information security policy, the BEST approach is to:

A. perform a vulnerability analysis

B. review the security of the application before implementation

C. integrate security functionality during the development stage

D. periodically audit the security of the application

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 321

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY driver for determining the classification of application systems?

A. The cost of repairing damage to system elements

B. The extent that compromise can affect revenue

C. The cost to implement regulatory requirements

D. Controlling access based on the need to know

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 322

Topic #: 1

[All CISM Questions]

Which of the following departments should be responsible for classifying customer relationship management (CRM) system data on a database server maintained by IT?

A. Sales

B. Information security

C. Human resources (HR)

D. IT

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 323

Topic #: 1

[All CISM Questions]

What is the role of the information security manager in finalizing contract negotiations with service providers?

A. To perform a risk analysis on the outsourcing process

B. To obtain a security standard certification from the provider

C. To update security standards for the outsourced process

D. To ensure that clauses for periodic audits are included

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 324

Topic #: 1

[All CISM Questions]

Which of the following is the BEST justification for making a revision to a password policy?

A. A risk assessment

B. Industry best practice

C. Audit recommendation

D. Vendor recommendation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 325

Topic #: 1

[All CISM Questions]

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

A. Incident response and recovery plans are documented in simple language

B. Copies of recovery and incident response plans are kept offsite

C. Teams and individuals responsible for recovery have been identified

D. Risk acceptance by the business has been documented.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 326

Topic #: 1

[All CISM Questions]

The BEST indicator the effectiveness of a security program conducted for users is an increase in the number of:

A. social engineering attempts reported to information security

B. requests for more security training information

C. participants in the security awareness program

D. threats detected by information security staff

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 327

Topic #: 1

[All CISM Questions]

When preventive controls to appropriately mitigate risk are not feasible, which of the following is the MOST important action for the information security manager?

A. Identifying unacceptable risk levels

B. Assessing vulnerabilities

C. Evaluating potential threats

D. Managing the impact

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 328

Topic #: 1

[All CISM Questions]

Which of the following is MOST effective in reducing the financial impact following a security breach leading to data disclosure?

A. Backup and recovery strategy

B. A business continuity plan (BCP)

C. A data loss prevention (DLP) solution

D. An incident response plan

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 329

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to prevent information security incidents?

A. Deploying intrusion detection tools in the network environment

B. Deploying a consistent incident response approach

C. Implementing a security information and event management (SIEM) tool

D. Implementing a security awareness training program for employees

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 330

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when updating procedures for managing security devices?

A. Updates based on changes in risk, technology, and process

B. Review and approval of procedures by management

C. Updates based on the organization's security framework

D. Notification to management of the procedural changes

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 331

Topic #: 1

[All CISM Questions]

Which of the following is the MAJOR advantage of conducting a post-incident review? The review:

A. helps develop business cases for security monitoring tools

B. provides continuous process improvement

C. facilitates reporting on actions taken during the incident process

D. helps identify current and desired level of risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 332

Topic #: 1

[All CISM Questions]

A modification to a critical system was not detected until the system was compromised. Which of the following will BEST help to prevent future occurrences?

A. Conducting continuous network monitoring

B. Improving the change control process

C. Conducting continuous risk assessments

D. Baselining server configurations

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 333

Topic #: 1

[All CISM Questions]

What would be the MAIN purpose of an immediate post-incident review after a comprehensive test of the incident response plan?

A. To reduce costs associated with incident response efforts

B. To determine ways to improve incident response plan processes

C. To document weaknesses for the next incident response plan test

D. To revalidate incident response plan activities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 334

Topic #: 1

[All CISM Questions]

An organization recently activated its business continuity plan (BCP). All employees were notified during the event, but some did not fully follow the communications plan. What is the BEST way to prevent a recurrence?

A. Perform tabletop testing with appropriate employees

B. Reprimand employees for not following the plan

C. Enhance external communication instructions in the BCP

D. Incorporate BCP communication expectations in job descriptions

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 335

Topic #: 1

[All CISM Questions]

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. Business impact analysis (BIA)

D. IT security risk and exposure

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 336

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to present the status of an information security program to senior management?

A. Detail latest security trends

B. Display concise dashboards

C. Provide detailed information regarding risk exposure

D. Report on root causes of security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 337

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY basis for an information security strategy?

A. Audit and regulatory requirements

B. Information security policies

C. The organization's vision and mission

D. Results of a comprehensive gap analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 338

Topic #: 1

[All CISM Questions]

What should an information security manager do FIRST to establish a roadmap for security investments?

A. Perform cost-benefit analyses of the investments

B. Gain a thorough understanding of the organization's operating processes

C. Establish business cases for proposed security investments

D. Ensure investments are strategically aligned with business objectives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 339

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to detect security incidents?

A. Analyze penetration test results

B. Analyze security anomalies

C. Analyze recent security risk assessments

D. Analyze vulnerability assessments

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 340

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY outcome of an information security program?

A. Threat reduction

B. Strategic alignment

C. Risk elimination

D. Cost reduction

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 341

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to help ensure web developers understand the growing severity of web application security risks?

A. Standardize secure web development practices

B. Integrate security into the early phases of the development life cycle

C. Incorporate security requirements into job descriptions

D. Implement a tailored security awareness training program

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 342

Topic #: 1

[All CISM Questions]

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

A. Need to know

B. Due diligence

C. Chain of custody

D. Preserving audit logs

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 343

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to detect information security incidents?

A. Establishing proper policies for response to threats and vulnerabilities

B. Performing regular testing of the incident response program

C. Providing regular and up-to-date training for the incident response team

D. Educating end users on threat awareness and timely reporting

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 344

Topic #: 1

[All CISM Questions]

During the due diligence phase of an acquisition, the MOST important course of action for an information security manager is to:

A. review the state of security awareness

B. review information security policies

C. perform a risk assessment

D. perform a gap analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 345

Topic #: 1

[All CISM Questions]

After the occurrence of a major information security incident, which of the following will BEST help an information security manager determine corrective actions?

A. Preserving the evidence

B. Performing an impact analysis

C. Calculating cost of the incident

D. Conducting a postmortem assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 346

Topic #: 1

[All CISM Questions]

An organization's information security manager reads on social media that a recently purchased vendor product has been compromised and customer data has been posted online. What should the information security manager do FIRST?

A. Activate the incident response program

B. Validate the risk to the organization

C. Perform a business impact analysis (BIA)

D. Notify local law enforcement agencies of a breach

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 347

Topic #: 1

[All CISM Questions]

Which of the following analyses will BEST identify the external influences to an organization's information security?

A. Threat analysis

B. Business impact analysis (BIA)

C. Gap analysis

D. Vulnerability analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 348

Topic #: 1

[All CISM Questions]

Which of the following would provide the MOST value to senior management when presenting the results of a risk assessment?

A. Mapping the risks to existing controls

B. Illustrating risk on a heat map

C. Providing a technical risk assessment report

D. Mapping the risks to the security classification scheme

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 349

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective approach to ensure IT processes are performed in compliance with the information security policies?

A. Ensuring that key controls are embedded in the processes

B. Providing information security policy training to the process owners

C. Allocating sufficient resources

D. Identifying risks in the processes and managing those risks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 350

Topic #: 1

[All CISM Questions]

An organization's human resources (HR) department is planning to migrate a legacy application to a new application in the cloud. What is the BEST way for the information security manager to support this effort?

A. Encrypt the data to the cloud so that the data is secure.

B. Conduct vulnerability scans on the cloud provider.

C. Update the policies to add controls for protecting the data.

D. Conduct a security assessment on the cloud provider.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 351

Topic #: 1

[All CISM Questions]

What is the PRIMARY goal of an incident management program?

A. Contain the incident

B. Communicate to external entities

C. Minimize impact to the organization

D. Identify root cause

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 352

Topic #: 1

[All CISM Questions]

Which of the following backup methods requires the MOST time to restore data for an application?

A. Disk mirroring

B. Differential

C. Incremental

D. Full backup

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 353

Topic #: 1

[All CISM Questions]

The PRIMARY advantage of performing black-box control tests as opposed to white-box control tests is that they:

A. require less IT staff preparation

B. identify more threats

C. simulate real-world attacks

D. cause fewer potential production issues

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 354

Topic #: 1

[All CISM Questions]

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

A. Lack of communication to affected users

B. Poor documentation of results and lessons learned

C. Lack of coordination among departments

D. Disruption to the production environment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 355

Topic #: 1

[All CISM Questions]

Inadvertent disclosure of internal business information on social media is BEST minimized by which of the following?

A. Implementing data loss prevention (DLP) solutions

B. Limiting access to social media sites

C. Developing social media guidelines

D. Educating users on social media risks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 356

Topic #: 1

[All CISM Questions]

Conflicting objectives are MOST likely to compromise the effectiveness of the information security process when information security management is:

A. partially staffed by external security consultants

B. combined with the change management function

C. reporting to the network infrastructure manager

D. outside of information technology

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 357

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to the effectiveness of an information security program?

A. Organizational culture

B. Risk management

C. IT governance

D. Security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 358

Topic #: 1

[All CISM Questions]

An information security manager has been asked to provide contract guidance from a security perspective for outsourcing the organization's payroll processing Which of the following is MOST important to address?

A. Vendor compliance with the most stringent data security regulations

B. Vendor compliance with the organization's information security policies

C. Vendor compliance with organizational service level agreement (SLA) requirements

D. Vendor compliance with recognized industry security standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 359

Topic #: 1

[All CISM Questions]

Which of the following should include contact information for representatives of equipment and software vendors?

A. Business continuity plan (BCP)

B. Service level agreements (SLAs)

C. Information security program charter

D. Business impact analysis (BIA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 360

Topic #: 1

[All CISM Questions]

Organization A offers e-commerce services and uses secure transport protocol! to protect Internet communication. To confirm communication with Organization A, which of the following would be the BEST for a client to verify?

A. The certificate of the e-commerce server

B. The browser's indication of SSL use

C. The IP address of the e-commerce server

D. The URL of the e-commerce server

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 361

Topic #: 1

[All CISM Questions]

During the eradication phase of an incident response, it is MOST important to:

A. identify the root cause

B. restore from the most recent backup

C. notify affected users

D. wipe the affected system

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 362

Topic #: 1

[All CISM Questions]

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. Identify and assess the risk in the context of business objectives

B. Consult with IT staff and assess the risk based on their recommendations

C. Update the security policy based on the regulatory requirements

D. Propose relevant controls to ensure the business complies with the regulation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 363

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST once a cybersecurity attack has been confirmed?

A. Isolate the affected system

B. Power down the system

C. Notify senior management

D. Contact legal authorities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 364

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST course of action to gain approval for investment in a technical control?

A. Calculate the exposure factor

B. Perform a cost-benefit analysis

C. Conduct a risk assessment

D. Conduct a business impact analysis (BIA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 365

Topic #: 1

[All CISM Questions]

Which of the following is an important criterion for developing effective key risk indicators (KRIs) to monitor information security risk?

A. The indicator should provide a retrospective view of risk impacts and be measured annually

B. The indicator should focus on IT and accurately represent risk variances

C. The indicator should align with key performance indicators (KPIs) and measure root causes of process performance issues

D. The indicator should possess a high correlation with a specific risk and be measured on a regular basis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 366

Topic #: 1

[All CISM Questions]

A health care organization's information security manager is notified of a possible breach of critical patient data involving a large volume of records. What should the information security manager do FIRST?

A. Notify health care regulators

B. Escalate the breach to senior management

C. Validate whether the breach occurred

D. Assess the possible impact of the breach.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 367

Topic #: 1

[All CISM Questions]

Which of the following presents the GREATEST risk associated with the use of an automated security information and event management (SIEM) system?

A. Low number of false negatives

B. High number of false negatives

C. Low number of false positives

D. High number of false positives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 368

Topic #: 1

[All CISM Questions]

Of the following, who should the security manager consult FIRST when determining the severity level of a security incident involving a third-party vendor?

A. Risk manager

B. Business partners

C. IT process owners

D. Business process owners

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 369

Topic #: 1

[All CISM Questions]

Recommendations for enterprise investment in security technology should be PRIMARILY based on:

A. availability of financial resources

B. alignment with business needs

C. the organization's risk tolerance

D. adherence to international standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 370

Topic #: 1

[All CISM Questions]

When implementing a security policy for an organization handling personally identifiable information (PII), the MOST important objective should be:

A. strong encryption

B. regulatory compliance

C. security awareness training

D. data availability

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 371
Topic #: 1
[All CISM Questions]

An information security manager has received confirmation that the organization's e-commerce website was breached, exposing customer information. What should be done FIRST?

A. Inform affected customers

B. Perform a vulnerability assessment

C. Execute the incident response plan

D. Take the affected systems offline

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 372

Topic #: 1

[All CISM Questions]

Which of the following would be MOST useful when illustrating to senior management the status of a recently implemented information security governance framework?

A. Periodic testing results

B. A risk assessment

C. A maturity model

D. A threat assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 373

Topic #: 1

[All CISM Questions]

An organization that has outsourced its incident management capabilities just discovered a significant privacy breach by an unknown attacker. Which of the following is the MOST important action of the information security manager?

A. Follow the outsourcer's response plan

B. Refer to the organization's response plan

C. Notify the outsourcer of the privacy breach

D. Alert the appropriate law enforcement authorities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 374

Topic #: 1

[All CISM Questions]

Which of the following would BEST support an information security manager's efforts to obtain management approval for an identity and access management (IAM) system implementation?

A. A recent security incident involving access authorization

B. An established security policy with access management requirements

C. A third-party audit finding based on regulatory requirements

D. A business case proposal for the solution

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 375

Topic #: 1

[All CISM Questions]

Internal audit has reported a number of information security issues that are not in compliance with regulatory requirements. What should the information security manager do FIRST?

A. Create a security exception

B. Assess the risk to business operations

C. Perform a vulnerability assessment

D. Perform a gap analysis to determine needed resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 376

Topic #: 1

[All CISM Questions]

An organization is about to purchase a rival organization. The PRIMARY reason for performing information security due diligence prior to making the purchase is to:

A. determine the security exposures

B. assess the ability to integrate the security department operations

C. ensure compliance with international standards

D. evaluate the security policy and standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 377

Topic #: 1

[All CISM Questions]

When considering whether to adopt bring your own device (BYOD), it is MOST important for the information security manager to ensure that:

A. the applications are tested prior to implementation

B. security controls are applied to each device when joining the network

C. users have read and signed acceptable use agreements

D. business leaders have an understanding of security risks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 378

Topic #: 1

[All CISM Questions]

The security baselines of an organization should be based on:

A. procedures.

B. standards.

C. policies.

D. guidelines.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 379

Topic #: 1

[All CISM Questions]

Which of the following would be MOST effective in changing the security culture and behavior of staff?

A. Promoting the information security mission within the enterprise

B. Enforcing strict technical information security controls

C. Auditing compliance with the information security policy

D. Developing procedures to enforce the information security policy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 380

Topic #: 1

[All CISM Questions]

Which of the following MUST be performed once risk has been accepted?

A. Reassess the risk on a regular basis.

B. Calculate the business impact of acceptance.

C. Flag the risk to avoid future reassessment.

D. Remove the risk from the risk register.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 381

Topic #: 1

[All CISM Questions]

Which of the following is the FIRST step in developing a business continuity plan (BCP)?

A. Identify critical business processes.

B. Determine the business recovery strategy

C. Determine available resources

D. Identify the applications with the shortest recovery time objectives (RTOs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 382

Topic #: 1

[All CISM Questions]

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

A. developing a security program that meets global and regional requirements.

B. ensuring effective communication with local regulatory bodies.

C. monitoring compliance with defined security policies and standards.

D. using industry best practice to meet local legal regulatory requirements.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 383

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when defining security configuration baselines?

A. The baselines address applicable regulatory standards.

B. The baselines are proportionate to risk.

C. The baselines address known system vulnerabilities.

D. The baselines align with lines of business.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 384

Topic #: 1

[All CISM Questions]

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

A. normal network behavior and using it as a baseline for measuring abnormal activity.

B. abnormal network behavior and using it as 4 baseline for measuring normal activity.

C. abnormal network behavior and issuing instructions to the firewall to drop rogue connections.

D. attack pattern signatures from historical data.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 385

Topic #: 1

[All CISM Questions]

Which of the following factors would have the MOST significant impact on an organization's information security governance model?

A. Corporate culture

B. Outsourced processes

C. Number of employees

D. Security budget

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 386

Topic #: 1

[All CISM Questions]

A newly appointed information security manager of a retailer with multiple stores discovers an HVAC (heating, ventilation, and air conditioning) vendor has remote access to the stores to enable real-time monitoring and equipment diagnostics. Which of the following should be the information security manager's FIRST course of action?

A. Disconnect the real-time access.

B. Conduct a penetration test of the vendor.

C. Review the vendor contract.

D. Review the vendor's technical security controls.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 387

Topic #: 1

[All CISM Questions]

Reverse lookups can be used to prevent successful:

A. denial of service (DoS) attacks.

B. phishing attacks.

C. session hacking.

D. Internet protocol (IP) spoofing.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 388

Topic #: 1

[All CISM Questions]

A post-incident review revealed that key stakeholders took longer than acceptable to decide whether an application should be shut down following a security breach. Which of the following is management's BEST course of action to rectify this issue?

A. Improve incident response criteria.

B. Improve incident response testing.

C. Define incident classification.

D. Establish containment procedures.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 389

Topic #: 1

[All CISM Questions]

To help ensure that an information security training program is MOST effective, its contents should be:

A. aligned to business processes.

B. based on employees' roles.

C. based on recent incidents.

D. focused on information security policy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 390

Topic #: 1

[All CISM Questions]

A technical vulnerability assessment on a personnel information management server should be performed when:

A. the data owner leaves the organization unexpectedly

B. the number of unauthorized access attempts increases

C. changes are made to the system configuration

D. an unexpected server outage has occurred

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 391

Topic #: 1

[All CISM Questions]

An organization has purchased an Internet sales company to extend the sales department. The information security manager's FIRST step to ensure the security policy framework encompasses the new business model is to:

A. perform a gap analysis.

B. implement both companies' policies separately.

C. merge both companies' policies.

D. perform a vulnerability assessment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 392

Topic #: 1

[All CISM Questions]

Relationships between critical systems are BEST understood by:

A. performing a business impact analysis (BIA).

B. developing a system classification scheme.

C. evaluating key performance indicators (KPIs).

D. evaluating the recovery time objectives (RTOs).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 393

Topic #: 1

[All CISM Questions]

Determining the risk for a particular threat/vulnerability pair before controls are applied can be expressed as:

A. the likelihood of a given threat attempting to exploit a vulnerability.

B. the magnitude of the impact, should a threat exploit a vulnerability.

C. a function of the cost and effectiveness of controls over a vulnerability.

D. a function of the likelihood and impact, should a threat exploit a vulnerability.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 394

Topic #: 1

[All CISM Questions]

When making decisions on prioritizing risk mitigation activities, which of the following would provide senior management with the MOST comprehensive information?

A. Risk assessment report

B. Risk action plan

C. Risk register

D. Internal audit report

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 395

Topic #: 1

[All CISM Questions]

What is the PRIMARY benefit of using key performance indicators (KPIs) for information security risk management?

A. Set targets against which the organization's information security function can be evaluated.

B. Prevent potential undesirable events from affecting information security.

C. Identify risk events that have already occurred from affecting information security.

D. Establish the process for setting organizational objectives in light of information security risk.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 396

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when reporting on the status of information security activities?

A. The report is comprehensive

B. The report is updated on a regular basis

C. The report is tailored to stakeholder needs

D. The report structure is consistent with industry standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 397

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important element when developing an information security strategy?

A. Identifying and classifying information assets

B. Determining the needs of the business

C. Aligning to applicable laws and regulations

D. Determining the risk management methodology

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 398

Topic #: 1

[All CISM Questions]

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

A. Industry security standards

B. The organizational structure

C. The organization's risk tolerance

D. Information security awareness

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 399

Topic #: 1

[All CISM Questions]

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

A. Balanced scorecard

B. Benchmarking

C. Heat map

D. Risk matrix

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 400

Topic #: 1

[All CISM Questions]

An employee of an organization has reported losing a smartphone that contains sensitive information. The BEST step to address this situation is to:

A. remotely wipe the device.

B. terminate the device connectivity.

C. disable the user's access to corporate resources.

D. escalate to the user's management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 401

Topic #: 1

[All CISM Questions]

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

A. Defined levels of severity

B. Senior management commitment

C. A business continuity plan (BCP)

D. An established escalation process

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 402

Topic #: 1

[All CISM Questions]

During the response to a serious security breach, who is the BEST organizational staff member to communicate with external entities?

A. The resource designated by senior management

B. The incident response team leader

C. The resource specified in the incident response plan

D. A dedicated public relations spokesperson

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 403

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to demonstrate the alignment of the information security strategy with the business strategy?

A. Show the relationship between information security goals and corporate goals.

B. Compare the allocated budget for business with the information security budget.

C. Present senior management's approval of information security policies.

D. Provide evidence that information security is included in the change management process.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 404

Topic #: 1

[All CISM Questions]

A newly appointed information security manager has been asked to update all security-related policies and procedures that have been static for five years or more. What is the BEST next step?

A. To gain an understanding of the current business direction

B. To update in accordance with the best business practices

C. To perform a risk assessment of the current IT environment

D. To assess corporate culture

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 405

Topic #: 1

[All CISM Questions]

Implementing the principle of least privilege PRIMARILY requires the identification of:

A. job duties.

B. primary risk factors.

C. authentication controls.

D. data owners.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 406

Topic #: 1

[All CISM Questions]

Which of the following is MOST helpful in preventing cybersecurity incidents?

A. Testing the backup plan according to a defined schedule

B. Documenting and testing incident response plans

C. Delivering periodic end-user security awareness training

D. Implementing best practice password parameters

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 407

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when determining which type of failover site to employ?

A. Disaster recovery test results

B. Reciprocal agreements

C. Recovery time objectives (RTOs)

D. Data retention requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 408

Topic #: 1

[All CISM Questions]

A risk owner has accepted a large amount of risk due to the high cost of controls. Which of the following should be the information security manager's PRIMARY focus in this situation?

A. Conducting an independent review of risk responses

B. Establishing a strong ongoing risk monitoring process

C. Presenting the risk profile for approval by the risk owner

D. Updating the information security standards to include the accepted risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 409

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important constraint to be considered when developing an information security strategy?

A. Established security policies and standards

B. Information security architecture

C. Compliance with an international security standard

D. Legal and regulatory requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 410

Topic #: 1

[All CISM Questions]

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

A. Speed of implementation

B. Reduction in residual risk

C. Industry peer benchmarking

D. Security framework alignment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 411

Topic #: 1

[All CISM Questions]

Which of the following BEST facilitates the effective execution of an incident response plan?

A. The plan is based on industry best practice.

B. The incident response plan aligns with the IT disaster recovery plan (DRP).

C. The plan is based on risk assessment results.

D. The response team is trained on the plan.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 412

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY reason that an information security manager should restrict the use of generic administrator accounts in a multi-user environment?

A. To prevent accountability issues

B. To ensure segregation of duties is maintained

C. To ensure system audit trails are not bypassed

D. To prevent unauthorized user access

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 413

Topic #: 1

[All CISM Questions]

Which of the following documents should contain the INITIAL prioritization of recovery of services?

A. Threat assessment

B. IT risk analysis

C. Business impact analysis (BIA)

D. Business process map

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 414

Topic #: 1

[All CISM Questions]

The department head of application development has decided to accept the risks identified in a recent assessment. No recommendations will be implemented, even though the recommendations are required by regulatory oversight. What should the information security manager do NEXT?

A. Formally document the decision.

B. Review the regulations.

C. Review the risk monitoring plan.

D. Perform a risk reassessment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 415

Topic #: 1

[All CISM Questions]

A company has a remote office located in a different country. The company's chief information security officer (CISO) has just learned of a new regulatory requirement mandated by the country of the remote office. Which of the following should be the NEXT step?

A. Integrate new requirements into the corporate policies

B. Evaluate whether the new regulation impacts information security

C. Create separate security policies and procedures for the new regulation

D. Implement the requirement at the remote office location

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 416

Topic #: 1

[All CISM Questions]

When integrating security risk management into an organization it is MOST important to ensure:

A. the risk management methodology follows an established framework.

B. business units approve the risk management methodology.

C. the risk treatment process is defined.

D. information security policies are documented and understood.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 417

Topic #: 1

[All CISM Questions]

Mitigating technology risks to acceptable levels should be based PRIMARILY upon:

A. business process requirements.

B. business process reengineering.

C. legal and regulatory requirements.

D. information security budget.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 418

Topic #: 1

[All CISM Questions]

For the information security manager, integrating the various assurance functions of an organization is important PRIMARILY to enable:

A. consistent security.

B. a security-aware culture.

C. compliance with policy.

D. comprehensive audits.

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 419
Topic #: 1
[All CISM Questions]

An organization has concerns regarding a potential advanced persistent threat (APT). To ensure that the risk associated with this threat is appropriately managed, what should be the organization's FIRST action?

A. Implement additional controls.

B. Report to senior management.

C. Initiate incident response processes.

D. Conduct an impact analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 420

Topic #: 1

[All CISM Questions]

Which of the following roles is accountable for ensuring the impact of a new regulatory framework on a business system is assessed?

A. Senior management

B. Application owner

C. Legal representative

D. Information security manager

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 421

Topic #: 1

[All CISM Questions]

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. security objectives

C. cost-benefit analyses

D. benchmarking security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 422

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to reduce the risk associated with a successful social engineering attack targeting help desk staff?

A. Conduct security awareness training

B. Implement two-factor authentication

C. Block access to social media sites

D. Enforce role based access to help desk systems

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 423

Topic #: 1

[All CISM Questions]

During the implementation of a new system, which of the following processes proactively minimizes the likelihood of disruption unauthorized alterations and errors?

A. Password management

B. Version management

C. Change management

D. Configuration management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 424

Topic #: 1

[All CISM Questions]

When evaluating the risk from external hackers the maximum exposure time would be the difference between:

A. log refresh and restoration.

B. identification and resolution.

C. detection and response.

D. compromise and containment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 425

Topic #: 1

[All CISM Questions]

What should be the FIRST step when implementing data loss prevention (DLP) technology?

A. Build a business case

B. Perform due diligence with vendor candidates

C. Classify the organization's data

D. Perform a cost benefit analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 426

Topic #: 1

[All CISM Questions]

When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to:

A. develop effective escalation and response procedures

B. make tabletop testing more effective

C. adequately staff and train incident response teams

D. communicate the incident response process to stakeholders

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 427

Topic #: 1

[All CISM Questions]

A financial company executive is concerned about recently increasing cyberattacks and needs to take action to reduce risk. The organization would BEST respond by:

A. increasing budget and staffing levels tor the incident response team

B. revalidating and mitigating risks to an acceptable level

C. implementing an intrusion detection system (IDS)

D. testing the business continuity plan (BCP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 428

Topic #: 1

[All CISM Questions]

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

A. consultants review the information security governance framework

B. IS auditors are empowered to evaluate governance activities

C. a culture of legal and regulatory compliance is promoted by management

D. risk management is built into operational and strategic activities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 429

Topic #: 1

[All CISM Questions]

Which of the following should be an information security manager's FIRST course of action when developing an incident management and response plan?

A. Reassess management's risk appetite

B. Conduct a gap analysis

C. Update the current risk register

D. Revise the business continuity plan (BCP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 430

Topic #: 1

[All CISM Questions]

An information security manager has observed multiple exceptions for a number of different security controls. Which of the following should be the information security manager's FIRST course of action?

A. Prioritize the risk and implement treatment options

B. Report the noncompliance to the board of directors

C. Inform respective risk owners of the impact of exceptions

D. Design mitigating controls tor the exceptions

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 431

Topic #: 1

[All CISM Questions]

Who is accountable for ensuring proper controls are in place to address the confidentiality and availability of an information system?

A. Information order

B. Business manager

C. Senior management

D. Information security manager

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 432

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to help assure the integrity of an organization's accounting system?

A. Performing frequent security reviews of the audit log

B. Implementing two-factor authentication

C. Conducting an annual security audit of the system

D. Providing security awareness training to accounting staff

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 433

Topic #: 1

[All CISM Questions]

An organization faces severe fines and penalties if not in compliance with local regulatory requirements by an established deadline. Senior management has asked the information security manager to prepare an action plan to achieve compliance. Which of the following would provide the MOST useful information for planning purposes?

A. Results from a business impact analysts (BIA)

B. Results from a gap analysis

C. An inventory of security controls currently in place

D. Deadlines and penalties for noncompliance

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 434
Topic #: 1
[All CISM Questions]

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

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 435

Topic #: 1

[All CISM Questions]

The information security manager of a multinational organization has been asked to consolidate the information security policies of its regional locations. Which of the following would be of GREATEST concern?

A. Varying threat environments

B. Disparate reporting lines

C. Conflicting legal requirements

D. Differences in work culture

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 436

Topic #: 1

[All CISM Questions]

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

A. Management decision on asset value

B. Penetration testing on key systems

C. Nondisclosure agreements (NDA) with employees

D. Mapping security processes to baseline security standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 437

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST value provided by a security information and event management (SIEM) system?

A. Facilitating the monitoring of risk occurrences

B. Measuring impact of exploits on business processes

C. Maintaining a repository base of security policies

D. Redirecting event logs to an alternate location for business continuity plan (BCP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 438

Topic #: 1

[All CISM Questions]

A critical vulnerability is found on a server hosting multiple applications owned by different business units. One of the business units finds its hosted application will not function with the patch applied and chooses to accept the risk. Which of the following should be the information security manager s NEXT course of action?

A. Update the risk register

B. Develop a business case for compensating controls

C. Update the information security policy

D. Consult the incident management process

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 439

Topic #: 1

[All CISM Questions]

The MOST important element in achieving executive commitment to an information security governance program is:

A. identified business drivers.

B. a process improvement model.

C. established security strategies.

D. a defined security framework.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 440

Topic #: 1

[All CISM Questions]

Which of the following recovery approaches generally has the LOWEST periodic cost?

A. Shared contingency center

B. Reciprocal agreement

C. Redundant site

D. Cold site

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 441

Topic #: 1

[All CISM Questions]

Which of the following tasks should he performed once a disaster recovery plan (DRP) has been developed?

A. Identify recovery time objectives (RTOs)

B. Develop the test plan

C. Analyze the business impact

D. Define response team roles

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 442

Topic #: 1

[All CISM Questions]

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

A. Ensuring human safety

B. Securing critical information assets

C. Ensuring the reliability of backup data

D. Identifying critical business processes

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 443

Topic #: 1

[All CISM Questions]

Which of the following should be the FIRST step of incident response procedures?

A. Classify the event depending on severity and type

B. Perform a risk assessment to determine the business impact

C. Evaluate the cause of the control failure

D. Identify if there is a need for additional technical assistance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 444

Topic #: 1

[All CISM Questions]

Which of the following is the BEST method for reducing the risk of data loss due to phishing attacks?

A. Changing passwords frequently

B. Implementing data loss prevention

C. Using spam filtering solutions

D. Educating users

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 445

Topic #: 1

[All CISM Questions]

Which of the following tools provides an incident response team with the GREATEST insight into insider threat activity across multiple systems?

A. An identity and access management (IAM) system

B. A virtual private network (VPN) with multi-factor authentication

C. A security information and event management (SIEM) system

D. An intrusion prevention system (IPS)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 446

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to the effectiveness of an information security program?

A. The program is aligned to legal and regulatory requirements

B. The program is aligned to a security control framework

C. Annual audits of the program are conducted

D. Users are trained on security policies and procedures

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 447

Topic #: 1

[All CISM Questions]

Conducting a business impact analysis (BIA) BEST helps to identify:

A. asset inventory

B. mitigation costs

C. residual risk

D. system criticality

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 448

Topic #: 1

[All CISM Questions]

An employee who denies accusations of downloading inappropriate material to an organizational device has been discharged. In support of the disciplinary action the collection of legal evidence is required. Which of the following is the information security manager's BEST recommendation?

A. Delete all inappropriate material after taking a local copy

B. Create a forensic image of the original file system

C. Log in to the employee's device and create a local copy to USB drive

D. Rely on server backup allowing strict access control

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 449

Topic #: 1

[All CISM Questions]

An information security manager wants to implement a security information and event management (SIEM) system that will aggregate log data from all systems that control perimeter access. Which of the following would BEST support the business case for this initiative to senior management?

A. Industry examples of threats detected using a SIEM system

B. Alignment with industry best practices

C. Independent evidence of a SIEM system's ability to reduce risk

D. Metrics related to the number of systems to be consolidated

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 450

Topic #: 1

[All CISM Questions]

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

A. identify control improvements

B. identify vulnerabilities

C. re-evaluate the impact of incidents

D. identify the root cause

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 451

Topic #: 1

[All CISM Questions]

In a call center, the BEST reason to conduct a social engineering exercise is to:

A. gain funding for information security initiatives

B. identify candidates for additional security training

C. improve password policy

D. minimize the likelihood of successful attacks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 452

Topic #: 1

[All CISM Questions]

The PRIMARY purpose of a penetration test is to:

A. test network load capability

B. validate firewall and router configuration

C. provide assurance of the security of the network

D. identify vulnerabilities at a particular point in time

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 453

Topic #: 1

[All CISM Questions]

An information security policy was amended recently to support an organization's new information security strategy. Which of the following should be the information security manager's NEXT step?

A. Evaluate the alignment with business strategy

B. Update standards and procedures

C. Review technical controls

D. Refresh the security training program

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 454

Topic #: 1

[All CISM Questions]

Which of the following needs to be established FIRST in order to categorize data properly?

A. A data protection policy

B. A data flow diagram

C. A data classification framework

D. A data custodian

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 455

Topic #: 1

[All CISM Questions]

Which of the following is the BEST course of action when confidential information is inadvertently disseminated outside the organization?

A. Change the encryption keys

B. Declare an incident

C. Review compliance requirements

D. Communicate the exposure

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 456

Topic #: 1

[All CISM Questions]

An organization is performing an annual review of its risk landscape. Which of the following anticipated changes will have the MOST significant impact on the information security strategy?

A. The renewal and renegotiation of the organization's contract with its managed security services provider

B. Migration of personal data to a new database system on a different server platform

C. The expansion to an international location with unfamiliar security and privacy regulations

D. Replacement of the aging enterprise-wide core firewall infrastructure with a new solution from a different vendor

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 457

Topic #: 1

[All CISM Questions]

Which of the following provides the MOST assurance that a third-party hosting provider will be able to meet availability requirements?

A. The third party's business continuity plan (BCP)

B. The third party's incident response plan

C. Right-to-audit clause

D. Service level agreement (SLA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 458

Topic #: 1

[All CISM Questions]

An organization permits the storage and use of its critical and sensitive information on employee-owned smartphones. Which of the following is the BEST security control?

A. Monitoring now often the smartphone is used

B. Developing security awareness training

C. Requiring the backup of the organization s data by the user

D. Establishing the authority to remote wipe

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 459
Topic #: 1
[All CISM Questions]

A spear phishing attack was used to trick a user into installing a Trojan onto a workstation. Which of the following would have been MOST effective in preventing this attack from succeeding?

A. Application control
B. Website blocking
C. Internet filtering
D. Network encryption

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 460

Topic #: 1

[All CISM Questions]

An information security manager has been asked to provide regular status reports to senior management regarding the information security program. Which of the following would provide the MOST helpful information?

A. A list detailing the latest threats

B. Number of phishing incidents per month

C. Remediation activities performed

D. Key performance indicators (KPIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 461

Topic #: 1

[All CISM Questions]

Which of the following would be the GREATEST threat posed by a distributed denial of service (DDoS) attack on a public-facing web server?

A. Execution of unauthorized commands

B. Unauthorized access to resources

C. Defacement of website content

D. Prevention of authorized access

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 462

Topic #: 1

[All CISM Questions]

Which of the following is the BEST indication of information security strategy alignment with the business?

A. Number of business executives who have attended information security awareness sessions

B. Percentage of corporate budget allocated to information security initiatives

C. Percentage of information security incidents resolved within defined service level agreements (SLAs)

D. Number of business objectives directly supported by information security initiatives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 463

Topic #: 1

[All CISM Questions]

Which of the following would BEST mitigate accidental data loss events?

A. Enforce a data hard drive encryption policy

B. Conduct a data loss prevention audit

C. Conduct periodic user awareness training

D. Obtain senior management support for the information security strategy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 464

Topic #: 1

[All CISM Questions]

Which of the following is a PRIMARY function of an incident response team?

A. To provide a single point of contact for critical incidents

B. To provide a risk assessment for zero-day vulnerabilities

C. To provide a business impact analysis (BIA)

D. To provide effective incident mitigation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 465

Topic #: 1

[All CISM Questions]

Using which of the following metrics will BEST help to determine the resiliency of IT infrastructure security controls?

A. Percentage of outstanding high-risk audit issues

B. Number of incidents resulting in disruptions

C. Number of successful disaster recovery tests

D. Frequency of updates to system software

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 466

Topic #: 1

[All CISM Questions]

Which of the following is the MAIN reason for integrating an organization's incident response plan with its business continuity process?

A. Incidents can escalate into disasters needing proper response

B. Recovery time objectives (RTOs) need to be determined

C. Incidents will be reported more timely when categorized as a disaster

D. Integration of the plan will reduce resource costs to the organization

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 467

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY basis for a severity hierarchy for information security incident classification?

A. Legal and regulatory requirements

B. Root cause analysis results

C. Availability of resources

D. Adverse effects on the business

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 468

Topic #: 1

[All CISM Questions]

Which of the following would BEST enable the timely execution of an incident response plan?

A. Definition of trigger events

B. Centralized service desk

C. The introduction of a decision support tool

D. Clearly defined data classification process

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 469

Topic #: 1

[All CISM Questions]

Which of the following is the BEST approach to identify new security issues associated with IT systems and applications in a timely manner?

A. Requiring periodic security audits of IT systems and applications

B. Comparing current state to established industry benchmarks

C. Performing a vulnerability assessment for each change to IT systems

D. Integrating risk assessments into the change management process

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 470

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to include in an information security strategy?

A. Industry benchmarks

B. Stakeholder requirements

C. Risk register

D. Regulatory requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 471

Topic #: 1

[All CISM Questions]

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 integrity during analysis

B. provide backup in case of media failure

C. reinstate original data when accidental changes occur

D. validate the confidentiality during analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 472

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important issue in a penetration test?

A. Performing the test without the benefit of any insider knowledge

B. Having an independent group perform the test

C. Having a defined goal as well as success and failure criteria

D. Obtaining permission from audit

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 473
Topic #: 1
[All CISM Questions]

An organization has decided to conduct a postmortem analysis after experiencing a loss from an information security attack. The PRIMARY purpose of this analysis should be to:

A. evaluate the impact.

B. prepare for criminal prosecution.

C. document lessons learned.

D. update information security policies.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 474

Topic #: 1

[All CISM Questions]

When a critical system incident is reported, the FIRST step of the incident handler should be to:

A. power off the system.

B. determine the scope of the incident.

C. validate the incident.

D. notify the appropriate parties.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 475

Topic #: 1

[All CISM Questions]

A multinational organization is introducing a security governance framework. The information security manager's concern is that regional security practices differ.

Which of the following should be evaluated FIRST?

A. Training requirements of the framework

B. Global framework standards

C. Cross-border data mobility

D. Local regulatory requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 476

Topic #: 1

[All CISM Questions]

Several months after the installation of a new firewall with intrusion prevention features to block malicious activity, a breach was discovered that came in through the firewall shortly after installation. This breach could have been detected earlier by implementing firewall:

A. web surfing controls

B. packet filtering

C. application awareness

D. log monitoring

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 477

Topic #: 1

[All CISM Questions]

Which of the following BEST enables successful identification of a potential IT security incident?

A. Configuration management standards

B. Event correlation

C. Network intrusion detection systems (NIDS)

D. File integrity monitoring

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 478

Topic #: 1

[All CISM Questions]

Which of the following is MOST important when providing updates during a security incident?

A. Responding immediately to questions from the public

B. Validating the reliability of information prior to dissemination

C. Designating a communications representative

D. Ensuring timely incident information to internal stakeholders

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 479

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 480

Topic #: 1

[All CISM Questions]

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

A. focus on compliance

B. reiterate the necessity of security

C. promote the relevance and contribution of security

D. rely on senior management to enforce security

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 481

Topic #: 1

[All CISM Questions]

Which of the following is the BEST indication of a mature information security program?

A. Security spending is below budget.

B. Security incidents are managed properly.

C. Security resources are optimized.

D. Security audit findings are reduced.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 482

Topic #: 1

[All CISM Questions]

An organization recently updated and published its information security policy and standards. What should the information security manager do NEXT?

A. Update the organization's risk register.

B. Develop a policy exception process.

C. Communicate the changes to stakeholders.

D. Conduct a risk assessment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 483

Topic #: 1

[All CISM Questions]

Which type of recovery site is MOST reliable and can support stringent recovery requirements?

A. Cold site

B. Warm site

C. Mobile site

D. Hot site

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 484

Topic #: 1

[All CISM Questions]

Which of the following has the MOST influence on the information security investment process?

A. Security key performance indicators (KPIs)

B. Organizational risk appetite

C. IT governance framework

D. Information security policy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 485

Topic #: 1

[All CISM Questions]

An organization's information security manager is performing a post-incident review of a security incident in which the following events occurred:

- A bad actor broke into a business-critical FTP server by brute forcing an administrative password
- The third-party service provider hosting the server sent an automated alert message to the help desk, but was ignored
- The bad actor could not access the administrator console, but was exposed to encrypted data transferred to the server
- After three (3) hours, the bad actor deleted the FTP directory, causing incoming FTP attempts by legitimate customers to fail

Which of the following could have been prevented by conducting regular incident response testing?

A. Stolen data

B. The server being compromised

C. The brute force attack

D. Ignored alert messages

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 486

Topic #: 1

[All CISM Questions]

Which of the following is MOST important when designing an information security governance framework?

A. Assessing the availability of information security resources

B. Assessing the current state of information security

C. Aligning with the information security strategy

D. Aligning with industry best practice frameworks

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 487

Topic #: 1

[All CISM Questions]

A serious vulnerability was detected in a business application that can be exploited by external attackers to compromise the system. What is the information security manager's BEST course of action?

A. Implement temporary remediation.

B. Request an immediate shutdown of the application.

C. Report the risk to the business application owner.

D. Ask the business application owner to apply the fix immediately.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 488

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to consider when defining escalation processes for incident response procedures?

A. Key risk indicators (KRIs)

B. Business continuity plans (BCPs)

C. Recovery time objectives (RTOs)

D. Key performance indicators (KPIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 489

Topic #: 1

[All CISM Questions]

To optimize the implementation of information security governance in an organization, an information security manager should:

A. implement processes consistent with international standards.

B. utilize existing governance structures when possible.

C. ensure changes are consistent with existing standards.

D. make gradual changes to governance to minimize employee resistance.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 490

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY goal of information security?

A. Business alignment

B. Regulatory compliance

C. Data governance

D. Information management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 491

Topic #: 1

[All CISM Questions]

Which of the following clauses would represent the MOST significant potential exposure if included in a contract with a third-party service provider?

A. Provider responsibility in a disaster limited to best reasonable efforts

B. Provider liability for loss of data limited to cost of physical media

C. Audit rights limited to customer data and supporting infrastructure

D. Access to escrowed software restricted to specific conditions

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 492

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY basis for determining information security objectives?

A. Business strategy

B. Regulatory requirements

C. Information security strategy

D. Data classification

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 493

Topic #: 1

[All CISM Questions]

Which of the following is the BEST method to ensure compliance with password standards?

A. A user-awareness program

B. Implementing password-synchronization software

C. Using password-cracking software

D. Automated enforcement of password syntax rules

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 494

Topic #: 1

[All CISM Questions]

The PRIMARY purpose for deploying information security metrics is to:

A. ensure that technical operations meet specifications.

B. compare program effectiveness to benchmarks.

C. support ongoing security budget requirements.

D. provide information needed to make decisions.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 495

Topic #: 1

[All CISM Questions]

Which of the following would BEST demonstrate the status of an organization's information security program to the board of directors?

A. The information security operations matrix

B. Changes to information security risks

C. Information security program metrics

D. Results of a recent external audit

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 496

Topic #: 1

[All CISM Questions]

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

A. Restore the application and data from a forensic copy.

B. Install the OS, patches, and application from the original source.

C. Restore the OS, patches, and application from a backup.

D. Remove all signs of the intrusion from the OS and application.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 497

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST when informed that customer data has been breached within a third-party vendor's environment?

A. Communicate the breach to leadership.

B. Request and verify evidence of the breach.

C. Notify the incident response team.

D. Review vendor obligations in the contract.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 498

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST benefit of using cyber threat intelligence to improve an organization's patch management program?

A. It allows the organization to define its risk tolerance and appetite.

B. It identifies when to use workarounds to mitigate vulnerabilities rather than patching.

C. It reduces the number of patches the organization needs to apply.

D. It provides information about exploited vulnerabilities to expedite patching.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 499

Topic #: 1

[All CISM Questions]

Which of the following methods enables the MOST rigorous testing while avoiding the disruption of normal business operations?

A. Walk-through test

B. Full interruption test

C. Parallel test

D. Checklist review test

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 500

Topic #: 1

[All CISM Questions]

An empowered security steering committee has decided to accept a critical risk. Which of the following is the information security manager's BEST course of action?

A. Notify the chief risk officer (CRO) and internal audit.

B. Determine the impact to information security objectives.

C. Remove the specific risk item from the risk register.

D. Document the risk acceptance and justification.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 501

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY benefit of implementing an information security governance framework?

A. The framework provides a roadmap to maximize revenue through the secure use of technology.

B. The framework is able to confirm the validity of business goals and strategies.

C. The framework defines managerial responsibilities for risk impacts to business goals.

D. The framework provides direction to meet business goals while balancing risks and controls.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 502

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to prevent insider threats?

A. Implement strict security policies and password controls.

B. Conduct organization-wide security awareness training.

C. Enforce segregation of duties and least privilege access.

D. Implement logging for all access activities.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 503

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST to ensure a new critical cloud application can be supported by internal personnel?

A. Establish a capability maturity model.

B. Develop a training plan.

C. Conduct a risk assessment.

D. Perform a skills gap analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 504

Topic #: 1

[All CISM Questions]

An organization is conducting a post-incident review to determine the root cause of an information security incident. Which of the following situations would be MOST harmful to this investigation?

A. Unencrypted logs of the affected systems were saved on magnetic tapes.

B. Antivirus signature update processes failed on the affected systems.

C. Systems logs were cleared by the administrator to free up space on the affected systems.

D. The incident response plan has not been updated during the past year.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 505

Topic #: 1

[All CISM Questions]

When building support for an information security program, which of the following elements is MOST important?

A. Business impact analysis (BIA)

B. Identification of existing vulnerabilities

C. Threat analysis

D. Information risk assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 506

Topic #: 1

[All CISM Questions]

Capacity planning would prevent:

A. system downtime for scheduled security maintenance.

B. file system overload arising from distributed denial of service (DDoS) attacks.

C. application failures arising from insufficient hardware resources.

D. software failures arising from exploitation of buffer capacity vulnerabilities.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 507

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective way to ensure information security policies are understood?

A. Implement a whistle-blower program.

B. Document security procedures.

C. Include security responsibilities in job descriptions.

D. Provide regular security awareness training.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 508

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective method for testing an incident response plan?

A. Disaster recovery testing

B. Risk assessment

C. Tabletop exercises

D. Industry benchmarking

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 509

Topic #: 1

[All CISM Questions]

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. Request funding needed to resolve the top vulnerabilities.

B. Ensure a risk assessment is performed to evaluate the findings.

C. Report findings to senior management.

D. Ensure vulnerabilities found are resolved within acceptable timeframes.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 510

Topic #: 1

[All CISM Questions]

An information security team must obtain approval from the information security steering committee to implement a key control. Which of the following is the MOST important input to assist the committee in making this decision?

A. IT strategy

B. Security architecture

C. Risk assessment

D. Business case

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 511

Topic #: 1

[All CISM Questions]

What should a global information security manager do FIRST when informed that a new regulation with significant impact will go into effect soon?

A. Perform a vulnerability assessment.

B. Perform a business impact analysis (BIA).

C. Perform a privacy impact assessment.

D. Perform a gap analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 512

Topic #: 1

[All CISM Questions]

Which of the following will have the MOST negative impact to the effectiveness of incident response processes?

A. High organizational risk tolerance

B. Decentralized incident monitoring

C. Ambiguous severity criteria

D. Manual incident reporting processes

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 513

Topic #: 1

[All CISM Questions]

Which of the following tasks would provide a newly appointed information security manager with the BEST view of the organization's existing security posture?

A. Performing a business impact analysis (BIA)

B. Reviewing policies and procedures

C. Performing a risk assessment

D. Interviewing business managers and employees

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 514

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration when developing incident classification methods?

A. Data classification

B. Data owner input

C. Service level agreements (SLAs)

D. Business impact

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 515

Topic #: 1

[All CISM Questions]

Which of the following should be the PRIMARY goal of an information security manager when designing information security policies?

A. Minimizing the cost of security controls

B. Reducing organizational security risk

C. Improving the protection of information

D. Achieving organizational objectives

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 516

Topic #: 1

[All CISM Questions]

An organization has outsourced many application development activities to a third party that uses contract programmers extensively. Which of the following would provide the BEST assurance that the third party's contract programmers comply with the organization's security policies?

A. Perform periodic security assessments of the contractors' activities.

B. Conduct periodic vulnerability scans of the application.

C. Require annual signed agreements of adherence to security policies.

D. Include penalties for noncompliance in the contracting agreement.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 517

Topic #: 1

[All CISM Questions]

How does an organization's information security steering committee facilitate the achievement of information security program objectives?

A. Monitoring information security resources

B. Making decisions on security priorities

C. Enforcing regulatory and policy compliance

D. Evaluating information security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 518

Topic #: 1

[All CISM Questions]

Which of the following is the BEST reason to consolidate security operations teams across a global organization?

A. Compliance with regulatory requirements

B. Enhanced visibility of threats

C. Detection of fraud

D. Cost reduction

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 519

Topic #: 1

[All CISM Questions]

The business value of an information asset is derived from:

A. its replacement cost.

B. the risk assessment.

C. its criticality.

D. the threat profile.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 520

Topic #: 1

[All CISM Questions]

A business unit handles sensitive personally identifiable information (PII), which presents a significant financial liability to the organization should a breach occur. Which of the following is the BEST way to mitigate the risk to the organization?

A. Implementing audit logging on systems

B. Including indemnification into customer contracts

C. Contracting the process to a third party

D. Purchasing insurance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 521

Topic #: 1

[All CISM Questions]

Which of the following would be impacted the MOST by a business decision to move from traditional computing to cloud computing?

A. Security awareness

B. Security standards

C. Security policies

D. Security strategy

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 522

Topic #: 1

[All CISM Questions]

Key risk indicators (KRIs) are MOST effective when they:

A. are mapped to core strategic initiatives.

B. allow for comparison with industry peers.

C. are redefined on a regular basis.

D. assess progress toward declared goals.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 523

Topic #: 1

[All CISM Questions]

An organization's intrusion prevention system (IPS) detected and blocked an unusually large number of external intrusion attempts within a 24-hour period. Which of the following should be the information security manager's FIRST course of action?

A. Perform security assessments on Internet-facing systems.

B. Identify the source and nature of the attempts.

C. Review the server and firewall audit logs.

D. Report the issue to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 524

Topic #: 1

[All CISM Questions]

Which of the following should be the GREATEST consideration when determining the recovery time objective (RTO) for an in-house critical application, database, or server?

A. Direction from senior management

B. Results of recovery testing

C. Determination of recovery point objective (RPO)

D. Impact of service interruption

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 525

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY purpose of implementing information security standards?

A. To provide a basis for developing information security policies

B. To provide step-by-step instructions for performing security-related tasks

C. To provide management direction with a specific security objective

D. To establish a minimum acceptable security baseline

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 526

Topic #: 1

[All CISM Questions]

Which of the following should be the FIRST step in patch management procedures when receiving an emergency security patch?

A. Validate the authenticity of the patch.

B. Conduct comprehensive testing of the patch.

C. Schedule patching based on the criticality.

D. Install the patch immediately to eliminate the vulnerability.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 527

Topic #: 1

[All CISM Questions]

The MOST effective tools for responding to new and advanced attacks are those that detect attacks based on:

A. behavior analysis.

B. penetration testing.

C. signature analysis.

D. data packet analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 528

Topic #: 1

[All CISM Questions]

When developing security processes for handling credit card data on the business unit's information system, the information security manager should FIRST:

A. ensure that systems that handle credit card data are segmented.

B. review industry best practices for handling secure payments.

C. ensure alignment with industry encryption standards.

D. review corporate policies regarding credit card information.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 529

Topic #: 1

[All CISM Questions]

What is the PRIMARY objective of information security involvement in the change management process?

A. To narrow the threat landscape

B. To ensure changes are not applied without prior authorization

C. To reduce the likelihood of control failure

D. To meet obligations for regulatory and legal compliance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 530

Topic #: 1

[All CISM Questions]

Which of the following is MOST likely to trigger an update and revision of information security policies?

A. Engagement with a new service provider

B. Replacement of the information security manager

C. Attainment of business process maturity

D. Changes in the organization's risk appetite

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 531

Topic #: 1

[All CISM Questions]

A small organization with limited budget hires a new information security manager who finds the same IT staff member is assigned the responsibility of system administrator, security administrator, database administrator, and application administrator. What is the manager's BEST course of action?

A. Formally document IT administrator activities.

B. Automate user provisioning activities.

C. Maintain strict control over user provisioning activities.

D. Implement monitoring of IT administrator activities.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 532

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST when assessing conflicting requirements between the global organization's security standards and local regulations?

A. Conduct a gap analysis against local regulations.

B. Perform a cost-benefit analysis of compliance.

C. Create a local version of the organizational standards.

D. Prioritize the organizational standards over local regulations.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 533

Topic #: 1

[All CISM Questions]

Which of the following is the BEST method to reduce the risk of an information security breach due to spear phishing?

A. Implementing a vulnerability management program

B. Deploying an intrusion protection system (IPS)

C. Establishing a company-wide information security awareness plan

D. Reviewing log files daily to identify any suspicious activity

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 534

Topic #: 1

[All CISM Questions]

A desktop computer is being used to perpetrate a fraud, and data on the machine must be secured for evidence. Which of the following should be done FIRST?

A. Encrypt the content of the hard drive using a strong algorithm.

B. Obtain a hash of the desktop computer's internal hard drive.

C. Copy the data on the computer to an external hard drive.

D. Capture a forensic image of the computer.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 535

Topic #: 1

[All CISM Questions]

The PRIMARY purpose of an information security governance framework is to ensure that the information security strategy is an extension of:

A. organizational strategies.

B. information technology strategies.

C. formal enterprise architecture.

D. approved business cases.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 536

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important consideration for a global organization that is designing an information security awareness program?

A. National regulations

B. Program costs

C. Cultural backgrounds

D. Local languages

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 537
Topic #: 1
[All CISM Questions]

Changes have been proposed to a large organization's enterprise resource planning (ERP) system that would violate existing security standards. Which of the following should be done FIRST to address this conflict?

A. Perform a cost-benefit analysis

B. Calculate business impact levels.

C. Validate current standards.

D. Implement updated standards.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 538

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do NEXT after creating a roadmap to execute the strategy for an information security program?

A. Develop a project plan to implement the strategy

B. Obtain consensus on the strategy from the executive board

C. Define organizational risk tolerance

D. Review alignment with business goals

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 539
Topic #: 1
[All CISM Questions]

An organization has just updated its backup capability to a new cloud-based solution. Which of the following tests will MOST effectively verify this change is working as intended?

A. Simulation testing

B. Tabletop testing

C. Parallel testing

D. Black box testing

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 540

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important function of an information security steering committee?

A. Assigning data classifications to organizational assets

B. Defining security standards for logical access controls

C. Developing organizational risk assessment processes

D. Obtaining multiple perspectives from the business

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 541

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to obtain reliable information to help an incident response team maintain awareness of emerging security threats and vulnerabilities?

A. Subscribe to a reputed threat intelligence group.

B. Assign staff to engage with social media hacking groups.

C. Review alerts from a security information and event management (SIEM) system.

D. Implement vulnerability scanners.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 542

Topic #: 1

[All CISM Questions]

Which of the following is the MOST effective approach to ensure seamless integration between the business continuity plan (BCP) and the incident response plan?

A. The BCP manager is included in the core incident response team.

B. Criteria for escalating to the BCP manager are in the incident response plan.

C. Both response teams contain the same members.

D. Consistent event classifications are used in both plans.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 543

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST course of action when a potential business breach is discovered in a critical business system?

A. Update the incident response plan.

B. Inform affected stakeholders.

C. Inform IT management.

D. Implement mitigating actions immediately.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 544

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to include in a report of an organization's information security risk?

A. Control risk

B. Mitigated risk

C. Residual risk

D. Inherent risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 545

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST recommendation to senior management following a breach at the organization's Software as a Service (SaaS) vendor?

A. Engage legal counsel

B. Terminate the relationship with the vendor

C. Renegotiate the vendor contract

D. Update the vendor risk assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 546

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to consider when determining asset valuation?

A. Potential business loss

B. Asset classification level

C. Asset recovery cost

D. Cost of insurance premiums

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 547
Topic #: 1
[All CISM Questions]

Which of the following should an information security manager do FIRST to address the risk associated with a new third-party cloud application that will not meet organizational security requirements?

A. Restrict application network access temporarily.

B. Update the risk register.

C. Consult with the business owner.

D. Include security requirements in the contract.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 548

Topic #: 1

[All CISM Questions]

An event occurred that resulted in the activation of the business continuity plan (BCP). All employees were notified during the event, and they followed the plan. However, two major suppliers missed deadlines because they were not aware of the disruption. What is the BEST way to prevent a similar situation in the future?

A. Ensure service level agreements (SLAs) with suppliers are enforced.

B. Conduct a vulnerability assessment.

C. Perform testing of the BCP communication plan.

D. Provide suppliers with access to the BCP document.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 549

Topic #: 1

[All CISM Questions]

When performing a data classification project, an information security manager should:

A. assign information criticality and sensitivity.

B. identify information custodians.

C. identify information owners.

D. assign information access privileges.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 550

Topic #: 1

[All CISM Questions]

Which of the following provides the MOST comprehensive information related to an organization's current risk profile?

A. Gap analysis results

B. Risk register

C. Heat map

D. Risk assessment results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 551

Topic #: 1

[All CISM Questions]

Which of the following has the GREATEST impact on the viability of an information security roadmap?

A. Regulatory requirements

B. Management support

C. Threat landscape

D. Resource availability

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 552

Topic #: 1

[All CISM Questions]

An information security manager is recommending an investment in a new security initiative to address recently published threats. Which of the following is MOST important to include in the business case?

A. Alignment with the approved IT strategy

B. Potential impact of threat realization

C. Availability of resources to implement the initiative

D. Peer group threat intelligence report

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 553

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important output from a post-incident review?

A. Documentation of lessons learned

B. Repository of digital forensic artifacts

C. Revised business impact analysis (BIA)

D. Compilation of incident-related costs

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 554

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST benefit of using a network-based intrusion prevention system (IPS)?

A. The ability to review and monitor data streams by network segment

B. The ability to shut down or block suspicious connections

C. Increased visibility into user web surfing

D. Centralized controls for incident handling

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 555
Topic #: 1
[All CISM Questions]

What should be the GREATEST concern for an information security manager of a large multinational organization when outsourcing data processing to a cloud service provider?

A. Local laws and regulations

B. Backup and restoration of data

C. Vendor service level agreements (SLAs)

D. Independent review of the vendor

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 556

Topic #: 1

[All CISM Questions]

Which of the following should be an information security manager's MAIN concern if the same digital signing certificate is able to be used by two or more users?

A. Potential to decrypt digital hash values

B. Inability to validate identity of sender

C. Certificate alteration

D. Segregation of duties

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 557

Topic #: 1

[All CISM Questions]

Signature based anti-malware controls are MOST effective against:

A. poorly configured firewall rules.

B. reused virus code.

C. known threats.

D. zero-day exploits.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 558

Topic #: 1

[All CISM Questions]

Which of the following is the PRIMARY objective of a business impact analysis (BIA)?

A. Confirm control effectiveness.

B. Determine recovery priorities.

C. Define the recovery point objective (RPO).

D. Analyze vulnerabilities.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 559

Topic #: 1

[All CISM Questions]

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

A. has an insufficient key length.

B. cannot interoperate across product domains.

C. cannot encrypt attachments.

D. has no key-recovery mechanism.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 560

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important outcome of effective risk treatment?

A. Implementation of corrective actions

B. Elimination of risk

C. Timely reporting of incidents

D. Reduced cost of acquiring controls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 561

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to the successful management of an information security program?

A. Compliance with regulatory requirements

B. Adequate security budget

C. Support from key stakeholders

D. Continuous controls monitoring

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 562

Topic #: 1

[All CISM Questions]

A newly hired information security manager discovers that the cleanup of accounts for terminated employees happens only once a year. Which of the following should be the information security manager's FIRST course of action?

A. Design and document a new process.

B. Perform a risk assessment.

C. Report the issue to senior management.

D. Update the security policy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 563

Topic #: 1

[All CISM Questions]

Which of the following BEST conveys minimum information security requirements to an organization in alignment with policies?

A. Procedures

B. Regulations

C. Baselines

D. Standards

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 564

Topic #: 1

[All CISM Questions]

Which of the following security initiatives should be the FIRST step in helping an organization maintain compliance with privacy regulations?

A. Implementing a data classification framework

B. Implementing security information and event management (SIEM)

C. Installing a data loss prevention (DLP) solution

D. Developing security awareness training

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 565

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to consider when developing a business case to support the investment in an information security program?

A. Senior management support

B. Results of a risk assessment

C. Results of a cost-benefit analysis

D. Impact on the risk profile

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 566

Topic #: 1

[All CISM Questions]

The PRIMARY reason for using metrics as part of an information security program is to help management:

A. determine whether objectives are being met.

B. visualize security trends.

C. develop an information security baseline.

D. track financial impact of the program.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 567

Topic #: 1

[All CISM Questions]

After an information security incident has been detected and its priority established, which of the following should be the NEXT course of action?

A. Gathering evidence

B. Eradicating the incident

C. Performing a risk assessment

D. Containing the incident

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 568

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important input to the development of an effective information security strategy?

A. Well-defined security policies and procedures

B. Current and desired state of security

C. Business processes and requirements

D. Risk and business impact assessments

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 569

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to review following a security incident?

A. Incident response procedures

B. Response tools and techniques

C. Incident response plan

D. Lessons learned

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 570

Topic #: 1

[All CISM Questions]

Which of the following is necessary to ensure consistent protection for an organization's information assets?

A. Control assessment

B. Data ownership

C. Regulatory requirements

D. Classification mode

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 571

Topic #: 1

[All CISM Questions]

A new law requires an organization to implement specific security controls. Which of the following should the information security manager do FIRST?

A. Integrate the new requirements into the security policy.

B. Perform a gap analysis on the new requirements.

C. Develop a control implementation plan.

D. Assess the risk of noncompliance with the new requirements.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 572

Topic #: 1

[All CISM Questions]

Which of the following BEST demonstrates that security controls are effective?

A. Audit report

B. Tabletop simulation

C. Risk and control self-assessment

D. Business impact analysis (BIA) results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 573

Topic #: 1

[All CISM Questions]

Which of the following activities provides the GREATEST insight into the level of threat exposure within an IT environment?

A. Executing an organization-wide security audit

B. Performing penetration testing

C. Performing technical vulnerability assessments

D. Conducting a red team exercise

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 574

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to ensure when an organization is moving portions of its sensitive database to the cloud?

A. The conversion has been approved by the information security team.

B. A right to audit clause is included in the contract.

C. Input from data owners is included in the requirements definition.

D. Data encryption is used in the cloud hosting solution.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 575

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to determine the gap between the present and desired state of an information security program?

A. Determine whether critical success factors (CSFs) have been defined.

B. Review and update current operational procedures.

C. Perform a risk analysis for critical applications.

D. Conduct a capability maturity model evaluation.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 576

Topic #: 1

[All CISM Questions]

The PRIMARY goal of information security governance is to:

A. reduce risk to an acceptable level.

B. align with business processes.

C. align with business objectives.

D. establish a security strategy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 577

Topic #: 1

[All CISM Questions]

An information security manager of an e-commerce business is reviewing the results of a business continuity plan (BCP) review. Which of the following findings should be the MOST immediate concern?

A. The cost of a recent recovery test exceeded budget expectations.

B. The annual business impact analysis (BIA) has been delayed.

C. The business continuity plan (BCP) has not been recently tested.

D. The recovery time objective (RTO) was not met during a recent power outage.

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 578
Topic #: 1
[All CISM Questions]

If an organization does not have an information security governance framework in place, which of the following would BEST facilitate the adoption of a future governance program?

A. Audit recommendations

B. IT department support

C. Information security funding

D. Involvement of business stakeholders

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 579

Topic #: 1

[All CISM Questions]

Which of the following would provide the GREATEST assurance to management that information security incidents will be detected and contained in a timely manner without jeopardizing the organization's mission?

A. Network security penetration testing program

B. Continuous vulnerability scanning solution

C. Security information and event management (SIEM) system

D. Fully operational security operations center (SOC)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 580

Topic #: 1

[All CISM Questions]

Which of the following would BEST provide stakeholders with information to determine the appropriate response to a disaster?

A. Vulnerability assessment

B. SWOT analysis

C. Business impact analysis (BIA)

D. Risk assessment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 581

Topic #: 1

[All CISM Questions]

Which of the following provides the BEST guidance when establishing a security program?

A. Risk assessment methodology

B. Security audit report

C. Information security budget

D. Information security framework

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 582

Topic #: 1

[All CISM Questions]

Which of the following should be of MOST concern to an information security manager reviewing the organization's disaster recovery plan (DRP)?

A. Organization wide training for disaster recovery has not occurred.

B. The response team has contracted with an external consultant to support testing activities.

C. Six months have elapsed since the most recent test of the response plan.

D. The response plan document has not been updated with the latest notification list details.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 583

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST risk of centralized information security administration within a multinational organization?

A. Slower turnaround

B. Less uniformity

C. Less objectivity

D. Violation of local law

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 584

Topic #: 1

[All CISM Questions]

Which of the following would BEST enable an organization to aggregate information from different systems to allow for centralized categorization of incidents?

A. Intrusion detection system (IDS)

B. Application program interfaces (APIs)

C. Intrusion prevention system (IPS)

D. Security information and event management (SIEM)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 585

Topic #: 1

[All CISM Questions]

When preparing an information security policy for a global organization, how should an information security manager BEST address local legislation in multiple countries?

A. Rely on local interpretation of the global policy to comply with local legislation.

B. Create a policy exception process for each country.

C. Enforce the same global policy in every country.

D. Establish local policies for each country that supplement the global policy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 586

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important control to implement when senior managers use smartphones to access sensitive company information?

A. Centralized device administration

B. Remote wipe capability

C. Anti-malware on the devices

D. Strong passwords

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 587
Topic #: 1
[All CISM Questions]

Which of the following is the MOST appropriate resource to determine whether or not a particular solution should utilize encryption based on its location and data classification?

A. Guidelines

B. Procedures

C. Standards

D. Policies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 588

Topic #: 1

[All CISM Questions]

An organization that conducts business globally is planning to utilize a third-party service provider to process payroll information. Which of the following issues poses the GREATEST risk to the organization?

A. The third party has not provided evidence of compliance with local regulations where data is generated.

B. The third party does not have an independent assessment of controls available for review.

C. The third party's service level agreement (SLA) does not include guarantees of uptime.

D. The third-party contract does not include an indemnity clause for compensation in the event of a breach.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 589

Topic #: 1

[All CISM Questions]

The PRIMARY objective of timely declaration of a disaster is to:

A. ensure the continuity of the organization's essential services.

B. protect critical physical assets from further loss.

C. ensure engagement of business management in the recovery process.

D. assess and correct disaster recovery process deficiencies.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 590

Topic #: 1

[All CISM Questions]

Which of the following BEST enables the design of an effective incident escalation process?

A. A well-defined organizational hierarchy

B. Enforceable control baselines

C. A comprehensive risk register

D. Controls designed for defense in depth

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 591

Topic #: 1

[All CISM Questions]

An information security manager has been notified that two senior executives have the ability to elevate their own privileges in the corporate accounting system, in violation of policy. What is the FIRST step to address this issue?

A. Notify the CISO of the security policy violation.

B. Perform a system access review.

C. Perform a full review of all system transactions over the past 90 days.

D. Immediately suspend the executives' access privileges.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 592

Topic #: 1

[All CISM Questions]

Which of the following is MOST useful to display on a dashboard to demonstrate security performance?

A. Number of hours spent per vulnerability remediated

B. Number of vulnerabilities detected over time

C. Severity of currently unremediated vulnerabilities

D. Average time to identify vulnerabilities

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 593

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST when establishing an information security governance framework?

A. Gain an understanding of the business and cultural attributes.

B. Contract a third party to conduct an independent review of the program.

C. Conduct a cost-benefit analysis of the framework.

D. Evaluate information security tools and skills relevant for the environment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 594

Topic #: 1

[All CISM Questions]

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

A. Establish periodic senior management meetings.

B. Establish regular information security status reporting.

C. Establish an information security steering committee.

D. Establish business unit security working groups.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 595

Topic #: 1

[All CISM Questions]

Which type of incident response test is the MOST efficient way to verify that backup power generators are functioning?

A. Operational full test

B. Simulation failure test

C. Parallel recovery test

D. Full interruption test

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 596

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important action to prepare for a ransomware attack?

A. Back up data regularly and verify the integrity of backups.

B. Scan emails to detect threats and filter out executable files.

C. Configure access controls with least privilege in mind.

D. Execute operating systems and programs in a virtualized environment.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 597

Topic #: 1

[All CISM Questions]

Which of the following should be the MAIN outcome from monitoring key performance indicators (KPIs) for a corporate security management program?

A. A balanced scorecard

B. An effective security awareness program

C. Data for the organization to assess progress

D. Optimal level of value delivery

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 598

Topic #: 1

[All CISM Questions]

An organization is considering using a third party to host sensitive archived data. Which of the following is MOST important to verify before entering into the relationship?

A. Independent audits of the vendor's operations are regularly conducted.

B. The vendor's controls are in line with the organization's security standards.

C. The encryption keys are not provided to the vendor.

D. The vendor's data centers are in the same geographic region.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 599

Topic #: 1

[All CISM Questions]

When creating an incident response plan, which of the following is MOST important to include during the preparation phase of the plan's life cycle?

A. Communication plan

B. Response procedures

C. Risk management plan

D. Forensic analysis procedures

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 600

Topic #: 1

[All CISM Questions]

A software vendor has announced a zero-day vulnerability that exposes an organization's critical business systems. The vendor has released an emergency patch. Which of the following should be the information security manager's PRIMARY concern?

A. Ability to test the patch prior to deployment

B. Adequacy of the incident response plan

C. Availability of resources to implement controls

D. Documentation of patching procedures

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 601

Topic #: 1

[All CISM Questions]

What is the MOST important reason to regularly report information security risk to relevant stakeholders?

A. To enable risk-informed decision making

B. To reduce the impact of information security risk

C. To ensure information security controls are effective

D. To achieve compliance with regulatory requirements

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 602

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to ensure ongoing senior management commitment to an organization's information security strategy?

A. Effective and reliable security reporting

B. A well-defined information security control framework

C. A detailed and documented business impact analysis (BIA)

D. Strategic alignment to an industry framework

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 603
Topic #: 1
[All CISM Questions]

A penetration test of a new system has identified a number of critical vulnerabilities, jeopardizing the go-live date. The information security manager is asked by the system owner to approve an exception to allow the system to be implemented without fixing the vulnerabilities. Which of the following is the MOST appropriate course of action?

A. Implement a log monitoring process.

B. Perform a risk assessment.

C. Develop a set of compensating controls.

D. Approve and document the exception.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 604

Topic #: 1

[All CISM Questions]

Which of the following information security activities is MOST helpful to support compliance with information security policy?

A. Conducting information security awareness programs

B. Creating monthly trend metrics

C. Performing periodic IT reviews on new system acquisitions

D. Obtaining management commitment

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 605

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to determine following the discovery and eradication of a malware attack?

A. The creator of the malware

B. The malware entry path

C. The type of malware involved

D. The method of detecting the malware

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 606

Topic #: 1

[All CISM Questions]

Which of the following is MOST helpful in ensuring an information security governance framework continues to support business objectives?

A. A consistent risk assessment methodology

B. A monitoring strategy

C. An effective organizational structure

D. Stakeholder buy-in

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 607

Topic #: 1

[All CISM Questions]

Reviewing which of the following would be MOST helpful when a new information security manager is developing an information security strategy for a non-regulated organization?

A. Management's business goals and objectives

B. Strategies of other non-regulated companies

C. Industry best practices and control recommendations

D. Risk assessment results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 608

Topic #: 1

[All CISM Questions]

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

A. review the number of reported security incidents.

B. evaluate results of the most recent incident response test.

C. ensure established security metrics are reported.

D. assess progress of risk mitigation efforts.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 609

Topic #: 1

[All CISM Questions]

Information security controls should be designed PRIMARILY based on:

A. regulatory requirements.

B. a vulnerability assessment.

C. business risk scenarios.

D. a business impact analysis (BIA).

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 610
Topic #: 1
[All CISM Questions]

An organization involved in e-commerce activities operating from its home country opened a new office in another country with stringent security laws. In this scenario, the overall security strategy should be based on:

A. risk assessment results.

B. international security standards.

C. the most stringent requirements.

D. the security organization structure.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 611

Topic #: 1

[All CISM Questions]

An information security manager developing an incident response plan MUST ensure it includes:

A. critical infrastructure diagrams.

B. a business impact analysis (BIA).

C. criteria for escalation.

D. an inventory of critical data.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 612

Topic #: 1

[All CISM Questions]

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

A. Require staff to sign confidentiality agreements.

B. Require staff to participate in information security awareness training.

C. Communicate disciplinary processes for policy violations.

D. Include information security responsibilities in job descriptions.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 613

Topic #: 1

[All CISM Questions]

Security program development is PRIMARILY driven by which of the following?

A. Regulatory requirements

B. Business strategy

C. Risk appetite

D. Available resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 614

Topic #: 1

[All CISM Questions]

An organization has identified a risk scenario that has low impact to the organization but is very costly to mitigate. Which risk treatment option is MOST appropriate in this situation?

A. Transfer

B. Acceptance

C. Mitigation

D. Avoidance

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 615

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 616

Topic #: 1

[All CISM Questions]

The fundamental purpose of establishing security metrics is to:

A. adopt security best practices.

B. establish security benchmarks.

C. provide feedback on control effectiveness.

D. increase return on investment (ROI).

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 617

Topic #: 1

[All CISM Questions]

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

A. An organization has a decentralized data center that uses cloud services.

B. Operating systems are no longer supported by the vendor.

C. IT system clocks are not synchronized with the centralized logging server.

D. The patch management system does not deploy patches in a timely manner.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 618

Topic #: 1

[All CISM Questions]

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. Define information security requirements and processes.

D. Analyze the risks and propose mitigating controls.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 619

Topic #: 1

[All CISM Questions]

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

A. report the root cause to the board of directors.

B. isolate the affected network segment.

C. shut down the entire network.

D. assess whether personally identifiable information (PII) is compromised.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 620

Topic #: 1

[All CISM Questions]

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

A. Walk-through of the incident response plan

B. Black box penetration test

C. Simulated phishing exercise

D. Red team exercise

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 621

Topic #: 1

[All CISM Questions]

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

A. Cost-benefit analysis

B. SWOT analysis

C. Business process analysis

D. Business impact analysis (BIA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 622

Topic #: 1

[All CISM Questions]

Which of the following BEST enables an organization to appropriately prioritize information security-focused projects?

A. Return on investment (ROI)

B. Privacy compliance requirements

C. Organizational risk appetite

D. Historical security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 623

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST upon learning that some security hardening settings may negatively impact future business activity?

A. Document a security exception.

B. Reduce security hardening settings.

C. Perform a risk assessment.

D. Inform business management of the risk.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 624

Topic #: 1

[All CISM Questions]

Which of the following activities MUST be performed by an information security manager for change requests?

A. Assess impact on information security risk.

B. Perform penetration testing on affected systems.

C. Scan IT systems for operating system vulnerabilities.

D. Review change in business requirements for information security.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 625

Topic #: 1

[All CISM Questions]

The PRIMARY purpose for continuous monitoring of security controls is to ensure:

A. alignment with compliance requirements.

B. effectiveness of controls.

C. control gaps are minimized.

D. system availability.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 626

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important factor of a successful information security program?

A. The program follows industry best practices.

B. The program is based on a well-developed strategy.

C. The program is focused on risk management.

D. The program is cost-efficient and within budget.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 627

Topic #: 1

[All CISM Questions]

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

A. Security is a business product and not a process.

B. Effective security eliminates risk to the business.

C. Adopt a recognized framework with metrics.

D. Security supports and protects the business.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 628

Topic #: 1

[All CISM Questions]

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

A. regulatory requirements.

B. control framework.

C. best practices.

D. cost-benefit analysis.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 629

Topic #: 1

[All CISM Questions]

A high-risk issue is discovered during an information security risk assessment of a legacy application. The business is unwilling to allocate the resources to remediate the issue. Which of the following would be the information security manager's BEST course of action?

A. Document risk acceptance from the business.

B. Recommend discontinuing the use of the legacy application.

C. Design alternative compensating controls to reduce the risk.

D. Present the worst-case scenario related to the risk.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 630

Topic #: 1

[All CISM Questions]

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.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 631

Topic #: 1

[All CISM Questions]

Which of the following is the MOST important reason to document information security incidents that are reported across the organization?

A. Support business investments in security.

B. Evaluate the security posture of the organization.

C. Identify unmitigated risk.

D. Prevent incident recurrence.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 632

Topic #: 1

[All CISM Questions]

Which of the following is MOST important for building a robust information security culture within an organization?

A. Mature information security awareness training across the organization

B. Security controls embedded within the development and operation of the IT environment

C. Senior management approval of information security policies

D. Strict enforcement of employee compliance with organizational security policies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 633

Topic #: 1

[All CISM Questions]

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

A. Documenting multiple scenarios for the organization and response steps

B. Providing training from third-party forensics firms

C. Obtaining industry certifications for the response team

D. Conducting tabletop exercises appropriate for the organization

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 634

Topic #: 1

[All CISM Questions]

Which of the following metrics BEST measures the effectiveness of an organization's information security program?

A. Return on information security investment

B. Number of information security business cases developed

C. Reduction in information security incidents

D. Increase in risk assessments completed

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 635

Topic #: 1

[All CISM Questions]

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

A. Capturing full system images

B. Documenting analysis steps

C. Maintaining a chain of custody

D. Analyzing system memory

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 636

Topic #: 1

[All CISM Questions]

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

A. Unavailable or corrupt data backups

B. Ineffective alert configurations for backup operations

C. Lack of encryption for backup data in transit

D. Undefined or undocumented backup retention policies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 637

Topic #: 1

[All CISM Questions]

An organization is aligning its incident response capability with a public cloud service provider. What should be the information security manager's FIRST course of action?

A. Identify the skill set of the provider's incident response team.

B. Update the incident escalation process.

C. Evaluate the provider's audit logging and monitoring controls.

D. Review the provider's incident definitions and notification criteria.

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 638
Topic #: 1
[All CISM Questions]

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

A. Key risk indicators (KRIs)

B. Responsible entities

C. Compensating controls

D. Potential business impact

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 639

Topic #: 1

[All CISM Questions]

An information security team has discovered that users are sharing a login account to an application with sensitive information, in violation of the access policy. Business management indicates that the practice creates operational efficiencies. What is the information security manager's BEST course of action?

A. Present the risk to senior management.

B. Modify the policy.

C. Create an exception for the deviation.

D. Enforce the policy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 640

Topic #: 1

[All CISM Questions]

Which of the following should be the FIRST step to gain approval for outsourcing to address a security gap?

A. Perform a cost-benefit analysis.

B. Collect additional metrics.

C. Begin due diligence on the outsourcing company.

D. Submit funding request to senior management.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 641

Topic #: 1

[All CISM Questions]

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

A. Business impact analysis (BIA)

B. Risk assessment

C. Vulnerability assessment

D. Industry best practices

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 642

Topic #: 1

[All CISM Questions]

Which of the following BEST ensures timely and reliable access to services?

A. Authenticity

B. Availability

C. Nonrepudiation

D. Recovery time objective (RTO)

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 643
Topic #: 1
[All CISM Questions]

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. Deterrent

B. Detective

C. Preventive

D. Corrective

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 644

Topic #: 1

[All CISM Questions]

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

A. Internal security audit

B. Organizational risk appetite

C. External security audit

D. Business impact analysis (BIA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 645

Topic #: 1

[All CISM Questions]

Which of the following is an information security manager's BEST course of action when a threat intelligence report indicates a large number of ransomware attacks targeting the industry?

A. Assess the risk to the organization.

B. Review the mitigating security controls.

C. Notify staff members of the threat.

D. Increase the frequency of system backups.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 646

Topic #: 1

[All CISM Questions]

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

A. Security architects

B. End users

C. Corporate auditors

D. Process owners

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 647

Topic #: 1

[All CISM Questions]

Which risk is introduced when using only sanitized data for the testing of applications?

A. Unexpected outcomes may arise in production.

B. Data disclosure may occur during the migration event.

C. Breaches of compliance obligations will occur.

D. Data loss may occur during the testing phase.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 648

Topic #: 1

[All CISM Questions]

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

A. Legal and regulatory requirements

B. Likelihood of a disaster

C. Organizational tolerance to service interruption

D. Geographical location of the backup site

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 649

Topic #: 1

[All CISM Questions]

Which of the following should be done FIRST when developing an information security program?

A. Establish security policies.

B. Define the security strategy.

C. Approve security standards.

D. Set security baselines.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 650

Topic #: 1

[All CISM Questions]

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 logs.

C. perform a business risk assessment of the email filtering system.

D. test user knowledge of information security practices.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 651

Topic #: 1

[All CISM Questions]

Which of the following is MOST important to have in place to help ensure an organization's cybersecurity program meets the needs of the business?

A. Information security awareness training

B. Risk assessment program

C. Information security governance

D. Information security metrics

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 652

Topic #: 1

[All CISM Questions]

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

A. More visibility to the impact of disruptions

B. Ability to monitor and control incident management costs

C. Effective protection of information assets

D. Optimized allocation of recovery resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 653

Topic #: 1

[All CISM Questions]

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

A. Business continuity plan (BCP)

B. Information security plan

C. Incident response plan

D. Disaster recovery plan (DRP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 654

Topic #: 1

[All CISM Questions]

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

A. Organizational standards are enforced by technical controls.

B. Organizational standards are included in awareness training.

C. Organizational standards are required to be formally accepted.

D. Organizational standards are documented in operational procedures.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 655

Topic #: 1

[All CISM Questions]

Which of the following should an information security manager do FIRST when a mandatory security standard hinders the achievement of an identified business objective?

A. Recommend risk acceptance.

B. Perform a cost-benefit analysis.

C. Escalate to senior management.

D. Revisit the business objective.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 656

Topic #: 1

[All CISM Questions]

A business unit is not complying with a control implemented to mitigate risk because doing so impacts the ability to achieve business goals. When reporting the noncompliance to senior management, what would be the information security manager's BEST recommendation?

A. Accept the noncompliance.

B. Conduct a control assessment.

C. Implement compensating controls.

D. Educate the noncompliant users.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 657

Topic #: 1

[All CISM Questions]

Which of the following is MOST helpful for protecting an enterprise from advanced persistent threats (APTs)?

A. Updated security policies

B. Regular antivirus updates

C. Defined security standards

D. Threat intelligence

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 658

Topic #: 1

[All CISM Questions]

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

A. Previously reported incidents

B. Management support

C. Compliance with regulations

D. The definition of an incident

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 659

Topic #: 1

[All CISM Questions]

A strict new regulation is being finalized to address global concerns regarding cybersecurity. Which of the following should the information security manager do FIRST?

A. Monitor industry response to the regulation.

B. Seek legal counsel on the new regulation.

C. Validate the applicability of the regulation.

D. Escalate compliance risk to senior management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 660

Topic #: 1

[All CISM Questions]

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 underlying reason for the user error

B. The time and location that the breach occurred

C. Appropriate disciplinary procedures for user error

D. Evidence of previous incidents caused by the user

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 661

Topic #: 1

[All CISM Questions]

The BEST way to ensure that frequently encountered incidents are reflected in the user security awareness training program is to include:

A. responses to security questionnaires.

B. previous training sessions.

C. examples of help desk requests.

D. results of exit interviews.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 662

Topic #: 1

[All CISM Questions]

A risk assessment exercise has identified the threat of a denial of service (DoS) attack. Executive management has decided to take no further action related to this risk. The MOST likely reason for this decision is:

A. the cost of implementing controls exceeds the potential financial losses.

B. the risk assessment has not defined the likelihood of occurrence.

C. executive management is not aware of the impact potential.

D. the reported vulnerability has not been validated.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 663

Topic #: 1

[All CISM Questions]

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

A. An increase in the identification rate during phishing simulations

B. An increase in the speed of incident resolution

C. An increase in positive user feedback

D. An increase in the frequency of phishing tests

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 664

Topic #: 1

[All CISM Questions]

Penetration testing is MOST appropriate when a:

A. new system is about to go live.

B. security incident has occurred.

C. security policy is being developed.

D. new system is being designed.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 665

Topic #: 1

[All CISM Questions]

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

A. Mature change management processes

B. Unannounced testing

C. Well-defined security policies

D. Senior management support

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 666

Topic #: 1

[All CISM Questions]

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

A. ensure changes are properly documented.

B. advise on change-related risk.

C. identify changes to the information security policy.

D. ensure that changes are tested.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 667

Topic #: 1

[All CISM Questions]

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

A. Senior management

B. Information security manager

C. Process manager

D. IT manager

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 668

Topic #: 1

[All CISM Questions]

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

A. Encrypt all personal data stored on systems and networks.

B. Evaluate privacy technologies required for data protection.

C. Create an inventory of systems where personal data is stored.

D. Update disciplinary processes to address privacy violations.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 669

Topic #: 1

[All CISM Questions]

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

A. Transfer responsibility for incident response to the cloud provider.

B. Continue using the existing incident response procedures.

C. Revise incident response procedures to encompass the cloud environment.

D. Adopt the cloud provider's incident response procedures.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 670

Topic #: 1

[All CISM Questions]

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. Provide regular reporting on risk treatment to senior management.

C. Require steering committee approval of risk treatment plans.

D. Use quantitative risk assessment methods.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 671

Topic #: 1

[All CISM Questions]

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

A. An evaluation of the effectiveness of the information security strategy

B. Documentation of regulatory reporting requirements

C. A review of the forensics chain of custody

D. Evaluations of the adequacy of existing controls

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 672

Topic #: 1

[All CISM Questions]

An organization plans to leverage popular social network platforms to promote its products and services. Which of the following is the BEST course of action for the information security manager to support this initiative?

A. Conduct vulnerability assessments on social network platforms.

B. Assess the security risk associated with the use of social networks.

C. Establish processes to publish content on social networks.

D. Develop security controls for the use of social networks.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 673

Topic #: 1

[All CISM Questions]

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

A. Ensuring current documentation of security processes

B. Formalizing a security strategy and program

C. Developing an awareness program for staff

D. Establishing processes within the security operations team

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 674

Topic #: 1

[All CISM Questions]

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

A. Balanced scorecard

B. Risk profile

C. Business impact analysis (BIA)

D. Key performance indicators (KPIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 675

Topic #: 1

[All CISM Questions]

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. the formalized acceptance of risk analysis by management.

C. the reporting of consistent and periodic assessments of risks.

D. an annual loss expectancy (ALE) determined from the history of security events.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 676

Topic #: 1

[All CISM Questions]

An organization is going through a digital transformation process, which places the IT organization in an unfamiliar risk landscape. The information security manager has been tasked with leading the IT risk management process. Which of the following should be given the HIGHEST priority?

A. Identification of risk

B. Selection of risk treatment options

C. Analysis of control gaps

D. Design of key risk indicators (KRIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 677

Topic #: 1

[All CISM Questions]

Which of the following change management procedures is MOST likely to cause concern to the information security manager?

A. Users are not notified of scheduled system changes.

B. Fallback processes are tested the weekend before changes are made.

C. The development manager migrates programs into production.

D. A manual rather than an automated process is used to compare program versions.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 678

Topic #: 1

[All CISM Questions]

Which is the BEST method to evaluate the effectiveness of an alternate processing site when continuous uptime is required?

A. Full interruption test

B. Tabletop test

C. Parallel test

D. Simulation test

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 679

Topic #: 1

[All CISM Questions]

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

A. Job descriptions include requirements to read security policies.

B. Senior management supports the policies.

C. The policies are aligned to industry best practices.

D. The policies are updated annually.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 680

Topic #: 1

[All CISM Questions]

If civil litigation is a goal for an organizational response to a security incident, the PRIMARY step should be to:

A. capture evidence using standard server-backup utilities.

B. document the chain of custody.

C. reboot affected machines in a secure area to search for evidence.

D. contact law enforcement.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 681

Topic #: 1

[All CISM Questions]

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. business senior management.

B. the compliance officer.

C. the information security manager.

D. the chief risk officer (CRO).

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 682
Topic #: 1
[All CISM Questions]

In an organization with a rapidly changing environment, business management has accepted an information security risk. It is MOST important for the information security manager to ensure:

A. change activities are documented.

B. compliance with the risk acceptance framework.

C. the rationale for acceptance is periodically reviewed.

D. the acceptance is aligned with business strategy.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 683

Topic #: 1

[All CISM Questions]

Which of the following is the BEST course of action for an information security manager to align security and business goals?

A. Reviewing the business strategy

B. Conducting a business impact analysis (BIA)

C. Actively engaging with stakeholders

D. Defining key performance indicators (KPIs)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 684

Topic #: 1

[All CISM Questions]

What should be the information security manager's FIRST step when updating an information security program?

A. Review costs and benchmark them against industry norms.

B. Interview business unit managers and key stakeholders.

C. Identify program components that do not align with business objectives.

D. Re-evaluate the organization's business expectations and objectives.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 685

Topic #: 1

[All CISM Questions]

Which of the following defines the triggers within a business continuity plan (BCP)?

A. Disaster recovery plan (DRP)

B. Needs of the organization

C. Information security policy

D. Gap analysis

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 686

Topic #: 1

[All CISM Questions]

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. Initiate the organization's incident response process.

D. Report the situation to the business owner of the application.

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 687

Topic #: 1

[All CISM Questions]

Which of the following is the BEST indication of a successful information security culture?

A. The budget allocated for information security is sufficient

B. End users know how to identify and report incidents

C. Individuals are given roles based on job functions

D. Penetration testing is done regularly and findings remediated

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 688

Topic #: 1

[All CISM Questions]

Which of the following plans should be invoked by an organization in an effort to remain operational during a disaster?

A. Incident response plan

B. Disaster recovery plan (DRP)

C. Business contingency plan

D. Business continuity plan (BCP)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 689

Topic #: 1

[All CISM Questions]

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

A. Business impact analysis (BIA)

B. Information security policy

C. Security risk register

D. Enterprise architecture (EA)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 690

Topic #: 1

[All CISM Questions]

Which of the following is the BEST technical defense against unauthorized access to a corporate network through social engineering?

A. Requiring multifactor authentication

B. Requiring challenge/response information

C. Enforcing frequent password changes

D. Enforcing complex password formats

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 691

Topic #: 1

[All CISM Questions]

What is the BEST way to reduce the impact of a successful ransomware attack?

A. Include provisions to pay ransoms in the information security budget

B. Monitor the network and provide alerts on intrusions

C. Perform frequent backups and store them offline

D. Purchase or renew cyber insurance policies

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 692

Topic #: 1

[All CISM Questions]

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

A. Require users to acknowledge the acceptable use policy

B. Base mandatory review and exception approvals on residual risk

C. Require the steering committee to review exception requests

D. Base mandatory review and exception approvals on inherent risk

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 693

Topic #: 1

[All CISM Questions]

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

A. Defining security asset categorization

B. Assigning information asset ownership

C. Developing a records retention schedule

D. Defining information stewardship roles

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 694

Topic #: 1

[All CISM Questions]

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

A. Infrastructure as a Service (IaaS)

B. Software as a Service (SaaS)

C. Disaster Recovery as a Service (DRaaS)

D. Platform as a Service (PaaS)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 695

Topic #: 1

[All CISM Questions]

Which of the following is the GREATEST benefit of conducting an organization-wide security awareness program?

A. More security incidents are detected

B. Security behavior is improved

C. The security strategy is promoted

D. Fewer security incidents are reported

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 696

Topic #: 1

[All CISM Questions]

Which of the following is the FIRST step to establishing an effective information security program?

A. Assign accountability

B. Perform a business impact analysis (BIA)

C. Create a business case

D. Conduct a compliance review

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 697

Topic #: 1

[All CISM Questions]

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

A. Re-classify the data and increase the security level to meet business risk

B. Complete a risk assessment and refer the results to the data owners

C. Instruct the relevant system owners to reclassify the data

D. Refer the issue to internal audit for a recommendation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 698

Topic #: 1

[All CISM Questions]

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

A. Requiring security awareness training for vendor staff

B. Including service level agreements (SLAs) in vendor contracts

C. Performing integration testing with vendor systems

D. Establishing communication paths with vendors

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 699

Topic #: 1

[All CISM Questions]

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. Details from intrusion detection system (IDS) logs

D. Method of operation used by the attacker

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 700

Topic #: 1

[All CISM Questions]

Which of the following is MOST important for an information security manager to verify when selecting a third-party forensics provider?

A. Existence of a right to audit clause

B. Technical capabilities of the provider

C. Results of the provider's business continuity tests

D. Existence of the provider's incident response plan

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 701

Topic #: 1

[All CISM Questions]

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

A. Antivirus software

B. Log monitoring

C. Intrusion detection

D. Patch management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 702

Topic #: 1

[All CISM Questions]

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. Updating information security awareness materials

C. Implementing a honeypot environment

D. Implementing proactive systems monitoring

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 703

Topic #: 1

[All CISM Questions]

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

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 704

Topic #: 1

[All CISM Questions]

An organization recently outsourced the development of a mission-critical business application. Which of the following would be the BEST way to test for the existence of backdoors?

A. Perform security code reviews on the entire application

B. Scan the entire application using a vulnerability scanning tool

C. Monitor Internet traffic for sensitive information leakage

D. Run the application from a high-privileged account on a test system

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 705

Topic #: 1

[All CISM Questions]

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

A. The vendor must be able to amend data

B. The vendor must agree to the organization's information security policy

C. Data is encrypted in transit and at rest at the vendor site

D. Data is subject to regular access log review

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 706

Topic #: 1

[All CISM Questions]

When investigating an information security incident details of the incident should be shared:

A. widely to demonstrate positive intent

B. only as needed

C. only with management

D. only with internal audit

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 707

Topic #: 1

[All CISM Questions]

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

A. can see the overall impact to the business

B. are more objective than information security management

C. can balance the technical and business risks

D. have a better understanding of specific business needs

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 708

Topic #: 1

[All CISM Questions]

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. certification scope is relevant to the service being offered

B. certification will remain current through the life of the contract

C. current international standard was used to assess security processes

D. certification can be extended to cover the client's business

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 709

Topic #: 1

[All CISM Questions]

Which of the following service offerings in a typical Infrastructure as a Service (IaaS) model will BEST enable a cloud service provider to assist customers when recovering from a security incident?

A. Capability to take a snapshot of virtual machines

B. Capability of online virtual machine analysis

C. Availability of web application firewall logs

D. Availability of current infrastructure documentation

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 710

Topic #: 1

[All CISM Questions]

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

A. Chief information security officer (CISO)

B. Chief information officer (CIO)

C. Chief operating officer (COO)

D. Chief executive officer (CEO)

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 711

Topic #: 1

[All CISM Questions]

Which of the following BEST indicates the effectiveness of a recent information security awareness campaign delivered across the organization?

A. Increase in the frequency of security incident escalations

B. Reduction in the impact of security incidents

C. Decrease in the number of security incidents

D. Increase in the number of reported security incidents

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 712

Topic #: 1

[All CISM Questions]

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

A. Security key performance indicators (KPIs)

B. Senior management sponsorship

C. Regular security policy reviews

D. Project resource optimization

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 713

Topic #: 1

[All CISM Questions]

When designing a disaster recovery plan (DRP), which of the following MUST be available in order to prioritize system restoration?

A. Key performance indicators (KPIs)

B. Systems inventory

C. Recovery procedures

D. Business impact analysis (BIA) results

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 714

Topic #: 1

[All CISM Questions]

Which of the following factors has the GREATEST influence on the successful implementation of information security strategy goals?

A. Regulatory requirements

B. Compliance acceptance

C. Management support

D. Budgetary approval

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 715

Topic #: 1

[All CISM Questions]

Which of the following is the BEST approach for managing user access permissions to ensure alignment with data classification?

A. Delegate the management of access permissions to an independent third party

B. Review access permissions annually or whenever job responsibilities change

C. Lock out accounts after a set number of unsuccessful login attempts

D. Enable multi-factor authentication on user and admin accounts

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 716

Topic #: 1

[All CISM Questions]

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

A. A comprehensive risk assessment program for information security

B. The information security manager's knowledge of the business

C. Ongoing audits and addressing open items

D. Security staff with appropriate training and adequate resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 717

Topic #: 1

[All CISM Questions]

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

A. A change in IT management

B. A merger with another organization

C. A significant increase in reported incidents

D. An increase in industry threat level

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 718

Topic #: 1

[All CISM Questions]

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

A. Members represent functions across the organization

B. Members have knowledge of information security controls

C. Members are rotated periodically

D. Members are business risk owners

Show Suggested Answer

Actual exam question from Isaca's CISM
Question #: 719
Topic #: 1
[All CISM Questions]

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. follow the incident response plan

B. follow the business continuity plan (BCP)

C. conduct an incident forensic analysis

D. notify the business process owner

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 720

Topic #: 1

[All CISM Questions]

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. Maintain multiple offline backups

D. Perform integrity checks on backups

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 721

Topic #: 1

[All CISM Questions]

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

A. Unreliable delivery of hardware and software resources by a supplier

B. Unavailability of services provided by a supplier

C. Loss of customers due to unavailability of products

D. Compromise of critical assets via third-party resources

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 722

Topic #: 1

[All CISM Questions]

An information security manager learns through a threat intelligence service that the organization may be targeted for a major emerging threat. Which of the following is the information security manager's FIRST course of action?

A. Conduct an information security audit

B. Perform a gap analysis

C. Validate the relevance of the information

D. Inform senior management

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 723

Topic #: 1

[All CISM Questions]

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

A. Internal compliance requirements are being met

B. Regulatory requirements are being met

C. Risk management objectives are being met

D. Business needs are being met

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 724

Topic #: 1

[All CISM Questions]

The MOST important attribute of a security control is that it is:

A. auditable

B. measurable

C. scalable

D. reliable

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 725

Topic #: 1

[All CISM Questions]

Which of the following will BEST enable an effective information asset classification process?

A. Reviewing the recovery time objective (RTO) requirements of the asset

B. Assigning ownership

C. Including security requirements in the classification process

D. Analyzing audit findings

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 726

Topic #: 1

[All CISM Questions]

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. Run a virus scan on the endpoint device

B. Wipe and reset the endpoint device

C. Power off the endpoint device

D. Isolate the endpoint device

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 727

Topic #: 1

[All CISM Questions]

During which of the following phases should an incident response team document actions required to remove the threat that caused the incident?

A. Eradication

B. Identification

C. Containment

D. Post-incident review

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 728

Topic #: 1

[All CISM Questions]

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

A. Wipe the device remotely

B. Remove user's access to corporate data

C. Prevent the user from using personal mobile devices

D. Report the incident to the police

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 729

Topic #: 1

[All CISM Questions]

An organization has acquired a company in a foreign country to gain an advantage in a new market. Which of the following is the FIRST step the information security manager should take?

A. Evaluate the information security laws that apply to the acquired company

B. Apply the existing information security program to the acquired company

C. Merge the two existing information security programs

D. Determine which country's information security regulations will be used

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 730

Topic #: 1

[All CISM Questions]

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. Require disaster recovery documentation be stored with all key decision makers

B. Provide annual disaster recovery training to appropriate staff

C. Maintain an outsourced contact center in another country

D. Store disaster recovery documentation in a public cloud

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 731

Topic #: 1

[All CISM Questions]

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

A. Penetration test

B. A maturity model

C. Improved risk management

D. Business agility

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 732

Topic #: 1

[All CISM Questions]

When designing an information security risk monitoring framework, it is MOST important to ensure:

A. preservation of forensic evidence is enabled

B. the monitoring system is patched regularly

C. feedback is communicated to stakeholders

D. outlier events are escalated to system administrators

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 733

Topic #: 1

[All CISM Questions]

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

A. Adequate security funding

B. A robust incident response program

C. Strong senior management support

D. Computer-based training

Show Suggested Answer

Actual exam question from Isaca's CISM

Question #: 734

Topic #: 1

[All CISM Questions]

Which of the following is the BEST way to rigorously test a disaster recovery plan (DRP) for a mission-critical system without disrupting business operations?

A. Parallel testing

B. Simulation testing

C. Checklist review

D. Structured walk-through

Show Suggested Answer