Which of the following is the MOST important for an information security manager to consider when developing a new information security policy?

1. Alignment with industry standards
2. Information security budget allocation
3. Organizational goals and objectives
4. Organizational culture and complexity

Ans: C $$

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

1. Calculate the total cost of ownership (TCO).
2. Perform a cost-benefit analysis.
3. Conduct a feasibility study
4. Define the issues to be addressed.

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

1. Drafting information security policities in line with business objectives
2. Updating the information security threat profile
3. Developing an information security architecture
4. Approving business cases for information security initiatives

Ans : D $$

Which of the following defines the minimum security requirements that a specific system must meet?

1. Security procedure
2. Security baseline
3. Security guideline
4. Security policy

Ans: B $$ Security baseline.

Which of the following is the BEST control to minimize the risk associated with loss of information as a result of ransomware exploiting a zero-day vulnerability?

A A security operation centre

A Public key Infrastructure

A Patch management process

A data recovery process

Ans: A $$ data recovery process.

An inexperienced information security manager is relying on its internal audit department to design and implement key security controls. Which of the following is the GREATEST risk?

1. Conflict of interest
2. Violation of the audit charter
3. Inadequate implementation of controls
4. Inadequate audit skills.

Ans: C $$onflict of interest

What is the Primary purpose of communicating business impact to an incident response team?

1. To enable effective prioritization of incidents
2. To facilitate resource allocation to preventive measures
3. To provide information for communication of incidents
4. To provide monetary values for post-incident review

Ans: A $$

1 The use of a business case to obtain funding for an information security investment is MOST

effective when the business case: [43901]

A: realigns information security objectives to organizational strategy.

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

C: relates the investment to the organization's strategic plan.

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

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43901

2 Which of the following metrics would be considered an accurate measure of a information security

program's performance? [43902]

A: A combination of qualitative and quantitative trends that enable decision making.

B: The number of key risk indications (KRIs) identified, monitored, and acted upon.

C: A single numeric score derived from various measures assigned to the security program.

D: A collection of qualitative indicators that accurately measure security exceptions.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

F43902

3 Which of the following is the PRIMARY reason to conduct periodic business impact assessments?

[43903]

A: Improve the results of last business impact assessment

B: Update recovery objectives based on new risks

C: Decrease the recovery times

D: Meet the needs of the business continuity policy

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43903

4 The PRIMARY purpose of a security information and event management (SIEM) system is to:

[43904]

A: track ongoing incidents.

B: resolve incidents.

C: identify potential incidents.

D: provide status of incidents.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43904

5 Which of the following would BEST demonstrate the maturity level of an organization's security

incident response program? [43905]

A: An increase in the number of reported incidents.

B: Ongoing review and evaluation of the incident response team.

C: A documented and live-tested incident response process.

D: A decrease in the number of reported incidents.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43905

6 An information security manager has been made aware that some employees are discussing

confidential corporate business on social media sites. Which of the following is the BEST response

to this situation? [43906]

A: Scan social media sites for company-related information.

B: Block workplace access to social media sites and monitor employee usage.

C: Communicate social media usage requirements and monitor compliance.

D: Train employees how to set up privacy rules on social media sites.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43906

7 An information security manager is reviewing the organization's incident response policy affected

by a proposed public cloud integration. Which of the following will be the MOST difficult to resolve

with the cloud service provider? [43907]

A: Accessing information security event data

B: Obtaining physical hardware for forensic analysis

C: Defining incidents and notification criteria

D: Regular testing of incident response plan

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43907

8 In a large organization, which of the following is the BEST source for identifying ownership of a PC?

[43908]

A: Identify management system

B: User ID register

C: Domain name server (DNS) records

D: Asset management register

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43908

9 A multinational organization has developed a bring your own device (BYOD) policy that requires

the installation of mobile device management (MDM) software on personally owned devices.

Which of the following poses the GREATEST challenge for implementing the policy? [43909]

A: Translation and communication of policy

B: Varying employee data privacy rights

C: Differences in corporate cultures

D: Differences in mobile OS platforms

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43909

10 To minimize security exposure introduced by changes to the IT environment, which of the

following is MOST important to implement as part of change management? [43910]

A: Conducting a security risk assessment prior to go-live

B: Requiring approval by senior management

C: Performing post-change reviews before closing change tickets

D: Performing a business impact analysis (BIA) prior to implementation

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43910

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

[43911]

A: Defense in depth

B: Threat management

C: Vulnerability management

D: Increased security awareness

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43911

12 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? [43912]

A: Determine the cost to remediate the noncompliance.

B: Present the noncompliance risk to senior management.

C: Investigate alternative options to remediate the noncompliance.

D: Assess the business impact to the organization.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43912

13 The MOST important reason to maintain key risk indicators (KRIs) is that: [43913]

A: threat and vulnerabilities continuously evolve.

B: they are needed to verify compliance with laws and regulations.

C: management uses them to make informed business decisions.

D: they help assess the performance of the security program.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43913

14 The BEST way to encourage good security practices is to: [43914]

A: schedule periodic compliance audits.

B: discipline those who fail to comply with the security policy.

C: recognize appropriate security behavior by individuals.

D: publish the information security policy.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43914

15 Which of the following would be MOST effective in preventing malware from being launched

through an email attachment? [43915]

A: Up-to-date security policies

B: Security awareness training

C: Placing the e-mail serve on a screened subnet

D: A network intrusion detection system (NIDS)

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43915

16 Recovery time objectives (RTOs) are an output of which of the following? [43916]

A: Business continuity plan

B: Disaster recovery plan

C: Service level agreement (SLA)

D: Business impact assessment (BIA)

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43916

17 Which of the following should an information security manager do FIRST after learning about a

new regulation that affects the organization? [43917]

A: Notify the affected business units.

B: Evaluate the changes with legal counsel.

C: Inform senior management of the new regulation.

D: Assess the noncompliance risk.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43917

18 Which of the following is the MOST important function of information security? [43918]

A: Identifying system vulnerabilities

B: Reducing the financial impact of security breaches

C: Preventing security incidents

D: Managing risk to the organization

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43918

19 Which of the following is the MOST important security consideration when using infrastructure as a

Service (IaaS)? [43919]

A: Segmentation among tenants

B: User access management

C: Backup and recovery strategy

D: Compliance with internal standards

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43919

20 Which of the following metrics would provide management with the useful information about the

progress of a security awareness program? [43920]

A: Increased number of downloads of the organization's security policy

B: Increased reported of security incidents

C: Completion rate of user awareness training within each business unit

D: Decreased number of security incidents

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43920

21 Which of the following is the PRIMARY reason to avoid alerting certain users of an upcoming

penetration test? [43921]

A: To evaluate detection and response capabilities

B: To prevent exploitation by malicious parties

C: To aid in the success of the penetration

D: To reduce the scope and duration of the test

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43921

22 Ensuring that activities performed by outsourcing providers comply with information security

policies can BEST be accomplished through the use of: [43922]

A: service level agreements.

B: independent audits.

C: explicit contract language.

D: local regulations.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43922

23 An organization is considering the purchase of a competitor. To determine the competitor's

security posture, the BEST course of action for the organization's information security manage

would be to: [43923]

A: assess the security policy of the competitor.

B: assess the key technical controls of the competitor.

C: conduct a penetration test of the competitor.

D: perform a security gap analysis on the competitor.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43923

24 After undertaking a security assessment of a production system, the information security manager

is MOST likely to: [43924]

A: inform the system owner of any residual risks and propose measures to reduce them.

B: establish an overall security program that minimizes the residual risks of that production system.

C: inform the IT manager of the residual risks and propose measures to reduce them.

D: inform the development team of any residual risks and together formulate risk reduction

measures.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43924

25 For an organization with a large and complex IT infrastructure, which of the following elements of a

disaster recovery hot site service will require the closest monitoring? [43925]

A: Employee access

B: Audit rights

C: Systems configurations

D: Number of subscribers

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43925

26 Which of the following is MOST critical to the successful implementation of information security

within an organization? [43926]

A: Strong risk management skills exist within the information security group.

B: The information security manager is responsible for setting information security policy.

C: Budget is allocated for information security tools.

D: Security is effectively marketed to all managers and employees.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43926

27 What should be an information security manager's FIRST course of action when an organization is

subject to a new regulatory requirement? [43927]

A: Perform a gap analysis

B: Complete a control assessment

C: Submit a business case to support compliance

D: Update the risk register

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43927

28 The BEST way to obtain funding from senior management for a security awareness program is to:

[43928]

A: demonstrate that the program will adequately reduce risk.

B: produce an impact analysis report of potential breaches.

C: meet regulatory requirements.

D: produce a report of organizational risks.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43928

29 Which of the following is the PRIMARY reason an information security strategy should be deployed

across an organization? [43929]

A: To ensure that management's intent is reflected in security activities

B: To ensure that employees adhere to security standards

C: To ensure that security-related industry best practices are adopted

D: To ensure that the business complies with security regulations

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43929

30 Which of the following provides the BEST opportunity to evaluate the capabilities of incident

response team members? [43930]

A: Black box penetration test

B: Breach simulation exercise

C: Tabletop test

D: Disaster recovery exercise

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43930

31 Which of the following is MOST helpful when justifying the funding required for a compensating

control? [43931]

A: Business impact analysis (BIA)

B: Risk analysis

C: Business case

D: Threat assessment

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43931

32 Which of the following presents the GREATEST information security concern when deploying an

identity and access management solution? [43932]

A: Complying with the human resource policy

B: Supporting multiple user repositories

C: Supporting legacy applications

D: Gaining end user acceptance

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43932

33 Which of the following is the MOST important reason to document information security incidents

that are reported across the organization? [43933]

A: Prevent incident recurrence.

B: Identify unmitigated risk.

C: Support business investments in security.

D: Evaluate the security posture of the organization.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43933

34 When aligning an organization's information security program with other risk and control activities,

it is MOST important to: [43934]

A: ensure adequate financial resources are available.

B: have information security management report to the chief risk officer.

C: integrate security within the system development life cycle.

D: develop an information security governance framework.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43934

35 Which of the following defines the triggers within a business continuity plan (BCP)? [43935]

A: Needs of the organization

B: Gap analysis

C: Disaster recovery plan

D: Information security policy

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43935

36 Which of the following is the BEST way to address any gaps identified during an outsourced

provider selection and contract negotiation process? [43936]

A: Implement compensating controls.

B: Make the provider accountable for security and compliance.

C: Perform continuous gap assessments.

D: Include audit rights in the service level agreement (SLA).

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43936

37 Which of the following is the BEST way to ensure information security metrics are meaningful?

[43937]

A: Aligning information security metrics with business drivers.

B: Correlating information security metrics to industry best practices.

C: Using a dashboard to present the information security metrics.

D: Requiring information security metrics to be approved by senior management.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43937

38 Risk management is MOST cost-effective [43938]

A: when performed on a continuous basis.

B: at the beginning of security program development.

C: while developing the business case for the security program.

D: when integrated into other corporate assurance functions.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43938

39 In addition to cost what is the BEST criteria for selecting countermeasures following a risk

assessment? [43939]

A: Maintenance requirements

B: Effectiveness of each option

C: Skill requirements for implementation

D: Effort of implementation

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43939

40 Which of the following would be the MOST effective incident response team structure for an

organization with a large headquarters and worldwide branch offices? [43940]

A: Outsourced

B: Coordinated

C: Decentralized

D: Centralized

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43940

41 When selecting risk response options to manage risk, an information security manager's MAIN

focus should be on reducing: [43941]

A: exposure to meet risk tolerance levels.

B: the likelihood of threat.

C: financial loss by transferring risk.

D: the number of security vulnerabilities.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43941

42 Which of the following functions is MOST critical when initiating the removal of system access for

terminated employees? [43942]

A: Help desk

B: Information security

C: Human resources

D: Legal

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43942

43 An information security manager learns that a departmental system is out of compliance with the

information security policy's authentication requirements. Which of the following should be the

information security manager's FIRST course of action? [43943]

A: Isolate the noncompliant system from the rest of the network.

B: Conduct an impact analysis to quantify the associated risk.

C: Request risk acceptance from senior management.

D: Submit the issue to the steering committee for escalation.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43943

44 Which of the following is the STRONGEST indication that senior management commitment to

information security is lacking within an organization? [43944]

A: A reduction in information security investment

B: Inconsistent enforcement of information security policies

C: The information security manager reports to the chief risk officer

D: A high level of information security risk acceptance

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43944

45 Which of the following is the MOST important consideration when deciding whether to continue

outsourcing to a managed security service provider? [43945]

A: The business need for the function

B: The ability to meet deliverables

C: The vendor's reputation in the industry

D: The cost of the services

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43945

46 An organization has determined that one of its web servers has been compromised. Which of the

following actions should be taken to preserve the evidence of the intrusion for forensic analysis

and potential litigation? [43946]

A: Run analysis tools to detect the source of the intrusion.

B: Reboot the server in a secure area to search for digital evidence.

C: Unplug the server from the power.

D: Restrict physical and logical access to the server.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43946

47 Which of the following would BEST help to identify vulnerabilities introduced by changes to an

organization's technical infrastructure? [43947]

A: An intrusion detection system

B: Established security baselines

C: Penetration testing

D: Log aggregation and correlation

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43947

48 An organization's security was compromised by outside attackers. The organization believed that

the incident was resolved. After a few days, the IT staff is still noticing unusual network traffic.

Which of the following is the BEST course of action to add [43948]

A: Identify potential incident impact.

B: Implement additional incident response monitoring tools.

C: Assess the level of the residual risk.

D: Initiate the incident response process.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43948

49 When implementing security architecture, an information security manager MUST ensure that

security controls: [43949]

A: form multiple barriers against threats.

B: are transparent.

C: are the least expensive.

D: are communicated through security policies.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43949

50 An organization has established information security policies, but the information security

manager has noted a large number of exception requests. Which of the following is the MOST likely

reason for this situation? [43950]

A: The information security policies lack alignment with corporate goals.

B: The information security program is not adequately funded.

C: The organization is operating in a highly regulated industry.

D: The information security policies are not communicated across the organization.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

51 To ensure IT equipment meets organizational security standards, the MOST efficient approach is

to: [43951]

A: assess security during equipment deployment.

B: ensure compliance during user acceptance testing.

C: assess the risks of all new equipment.

D: develop an approved equipment list.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43951

52 The PRIMARY reason for classifying assets is to: [43952]

A: balance asset value and protection measures.

B: inform senior management of the organization's risk posture.

C: identify low-value assets with insufficient controls.

D: establish clear lines of authority and ownership for the asset.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43952

53 Which of the following is the MOST important factor to ensure information security is meeting the

organization's objectives? [43953]

A: Internal audit's involvement in the security process

B: Implementation of a control self-assessment process

C: Establishment of acceptable risk thresholds

D: Implementation of a security awareness program

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43953

54 The BEST way to isolate corporate data stored on employee-owned mobile devices would be to

implement: [43954]

A: a sandbox environment

B: device encryption

C: two-factor authentication

D: a strong password policy

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43954

55 Which of the following is the BEST method to ensure that data owners take responsibility for

implementing information security processes? [43955]

A: Increase security awareness training.

B: Include security tasks into employee job descriptions.

C: Include membership on project teams.

D: Provide job rotation into the security organization.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43955

56 What is the MOST important role of an organization's data custodian in support of the information

security function? [43956]

A: Evaluating data security technology vendors

B: Assessing data security risks to the organization

C: Applying approved security policies

D: Approving access rights to departmental data

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43956

57 Reviewing which of the following would provide the GREATEST input to the asset classification

process? [43957]

A: Sensitivity of the data

B: Compliance requirements

C: Replacement cost of the asset

D: Risk assessment

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43957

58 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? [43958]

A: End user acceptance

B: Disparate device security / inconsistent device security

C: Mobile application control

D: Configuration management

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43958

59 In a large organization requesting outsourced services, which of the following contract clauses is

MOST important to the information security manager? [43959]

A: Compliance with security requirements

B: Frequency of status reporting

C: Nondisclosure clause

D: Intellectual property

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43959

60 An organization has an approved bring your own device (BYOD) program. Which of the following is

the MOST effective method to enforce application control on personal devices? [43960]

A: Implement a mobile device management (MDM) solution.

B: Implement a web application firewall.

C: Educate users regarding the use of approved applications.

D: Establish a mobile device acceptable use policy.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43960

61 Which of the following BEST promotes stakeholder accountability in the management of

information security risks? [43961]

A: Establishment of information ownership

B: Regular reviews for noncompliance

C: Establishment of security baselines

D: Targeted security procedures

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43961

62 When trying to integrate information security across an organization, the MOST important goal for

a governing body should be to ensure: [43962]

A: information security is treated as a business critical issue.

B: periodic information security audits are conducted.

C: funding is approved for requested information security projects.

D: the resources used for information security projects are kept to a minimum.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43962

63 An information security manager is developing a new information security strategy. Which of the

following functions would serve as the BEST resource to review the strategy and provide guidance

for business alignment? [43963]

A: The board of directors

B: Internal audit

C: The steering committee

D: The legal department

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43963

64 An organization has detected potential risk emerging from noncompliance with new regulations in

its industry. Which of the following is the MOST important reason to report this situation to senior

management? [43964]

A: The risk profile needs to be updated.

B: An external review of the risk needs to be conducted.

C: Specific monitoring controls need to be implemented.

D: A benchmark analysis needs to be performed.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43964

65 An organization plans to implement a document collaboration solution to allow employees to

share company information. Which of the following is the MOST important control to mitigate the

risk associated with the new solution? [43965]

A: Assign write access to data owners.

B: Allow a minimum number of users access to the solution.

C: Have data owners perform regular user access reviews.

D: Permit only non-sensitive information on the solution.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

66 Which of the following is MOST helpful for protecting an enterprise from advanced persistent

threats (APTs)? [43966]

A: Threat intelligence

B: Defined security standards

C: Updated security policies

D: Regular antivirus updates

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43966

67 What is the PRIMARY role of the information security manager in the process of information

classification within an organization? [43967]

A: Defining and ratifying the classification structure of information assets

B: Deciding the classification levels applied to the organization's information assets

C: Securing information assets in accordance with their classification

D: Checking if information assets have been classified properly

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43967

68 In a resource-restricted security program, which of the following approaches will provide the BEST

use of the limited resources? [43968]

A: Cross-training

B: Risk avoidance

C: Risk prioritization

D: Threat management

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43968

69 When integrating information security requirements into software development, which of the

following practices should be FIRST in the development lifecycle? [43969]

A: Source code review

B: Penetration testing

C: Dynamic code analysis

D: Threat modeling

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43969

70 Which of the following is the PRIMARY goal of a risk management program? [43970]

A: Manage compliance with organizational polices.

B: Implement preventive controls against threats.

C: Reduce the organization's risk appetite.

D: Manage the business impact of inherent risks.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43970

71 An organization has detected sensitive data leakage caused by an employee of a third-party

contractor. What is the BEST course of action to address this issue? [43971]

A: Activate the organization's incident response plan.

B: Limit access to the third-party contractor.

C: Include security requirements in outsourcing contracts.

D: Terminate the agreement with the third-party contractor.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43971

72 When considering whether to adopt a new information security framework, an organization's

information security manager should FIRST: [43972]

A: compare the framework with the current business strategy

B: perform a technical feasibility analysis

C: perform a financial viability study

D: analyze the framework's legal implications and business impact

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43972

73 Which of the following metrics provides the BEST indication of the effectiveness of a security

awareness campaign? [43973]

A: The number of reported security events

B: Percentage of users who have taken the courses

C: User approval rating of security awareness classes

D: Quiz sources for users who took security awareness classes

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43973

74 The MOST important reason for an information security manager to be involved in a new software

purchase initiative is to: [43974]

A: choose the software with the most control options.

B: provide input for user requirements.

C: ensure there is software escrow in place.

D: ensure the appropriate controls are considered.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43974

75 When granting a vendor remote access to a system, which of the following is the MOST important

consideration? [43975]

A: Password hashing

B: Multi-factor authentication

C: Hard drive encryption

D: Session monitoring

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

76 Which of the following is the BEST type of access control for an organization with employees who

move between departments? [43976]

A: Discretionary

B: Role-based

C: Mandatory

D: Identity

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43976

77 Vulnerability scanning has detected a critical risk in a vital business application. Which of the

following should the information security manager do FIRST? [43977]

A: Update the risk register.

B: Confirm the risk with the business owner.

C: Create an emergency change request.

D: Report the business risk to senior management.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43977

78 Which of the following threats is prevented by using token-based authentication? [43978]

A: Denial of service attack over the network

B: Password sniffing attack on the network

C: Man-in-the-middle attack on the client

D: Session eavesdropping attack on the network

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43978

79 Which of the following is the PRIMARY responsibility of the information security steering

committee? [43979]

A: Developing security policies aligned with the corporate and IT strategies

B: Reviewing business cases where benefits have not been realized

C: Identifying risks associated with new security initiatives

D: Developing and presenting business cases for security initiatives

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43979

80 Which of the following is MOST critical for an effective information security governance

framework? [43980]

A: Board members are committed to the information security program.

B: Information security policies are reviewed on a regular basis.

C: The information security program is continually monitored.

D: The CIO is accountable for the information security program.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43980

81 Inadvertent disclosure of internal business information on social media is BEST minimized by which

of the following? [43981]

A: Limiting access to social media sites

B: Developing social media guidelines

C: Educating users on social media risks

D: Implementing data loss prevention (DLP) solutions

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43981

82 Which of the following would BEST help an information security manager prioritize remediation

activities to meet regulatory requirements? [43982]

A: Alignment with the IT strategy

B: Annual loss expectancy (ALE) of noncompliance

C: Cost of associated controls

D: A capability maturity model matrix

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43982

83 Which of the following is MOST relevant for an information security manager to communicate to

business units? [43983]

A: Risk ownership

B: Business impact analysis (BIA)

C: Threat assessments

D: Vulnerability assessments

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43983

84 Which of the following defines the minimum security requirements that a specific system must

meet? [43984]

A: Security guideline

B: Security policy

C: Security baseline

D: Security procedure

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43984

85 Which of the following would be the MOST effective to mitigate the risk of data loss in the event of

a stolen laptop? [43985]

A: Providing end-user awareness training focused on travelling with laptops

B: Deploying end-point data loss prevention software on the laptop

C: Encrypting the hard drive

D: Utilizing a strong password

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

86 Which of the following BEST determine an information asset's classification? [43986]

A: Cost of producing the information asset

B: Directives from the data owner

C: Value of the information asset to competitors

D: Criticality to a business process

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43986

87 Which of the following is the BEST option for addressing regulations that will adversely the

allocation of information security program resources? [43987]

A: Delay implementation of compliance activities.

B: Conduct assessments for management decisions.

C: Determine compliance levels of peer organizations.

D: Prioritize compliance efforts based on probability.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43987

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

[43988]

A: Approving the purchase of information security technologies

B: Analyzing information security policy compliance reviews

C: Reviewing the information security strategy

D: Approving the information security awareness training strategy

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43988

89 When conducting a post-incident review, the GREATEST benefit of collecting mean time to

resolution (MTTR) data is the ability to: [43989]

A: reduce the costs of future preventive controls.

B: provide metrics for reporting to senior management.

C: verify compliance with the service level agreement (SLA).

D: learn of potential areas of improvement.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43989

90 An organization is planning to open a new office in another country. Sensitive data will be

routinely sent between the two offices. What should be the information security manager's FIRST

course of action? [43990]

A: Apply the current corporate security policies to the new office.

B: Encrypt the data for transfer to the head office based on security manager approval.

C: Update privacy policies to include the other country's laws and regulations.

D: Identify applicable regulatory requirements to establish security policies.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

91 Which of the following is the MOST important outcome of testing incident response plans? [43991]

A: An action plan is available for senior management.

B: Staff is educated about current threats.

C: Internal procedures are improved.

D: Areas requiring investment are identified.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43991

92 Which of the following BEST demonstrates alignment between information security governance

and corporate governance? [43992]

A: Average number of security incidents across business units

B: Number of vulnerabilities identified for high-risk information assets

C: Security project justifications provided in terms of business value

D: Mean time to resolution for enterprise-wide security incidents

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43992

93 The MAIN purpose of documenting information security guidelines for use within a large,

international organization is to: [43993]

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

B: ensure that all business units implement identical security procedures.

C: explain the organization's preferred practices for security.

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

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43993

94 In which of the following ways can an information security manager BEST ensure that security

controls are adequate for supporting business goals and objectives? [43994]

A: Enforcing strict disciplinary procedures in case of noncompliance

B: Using the risk management process

C: Reviewing results of the annual company external audit

D: Adopting internationally accepted controls

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43994

95 Which of the following is the BEST course of action for the information security manager when

residual risk is above the acceptable level of risk? [43995]

A: Defer to business management.

B: Carry out a risk assessment.

C: Perform a cost-benefit analysis.

D: Recommend additional controls.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

96 Which of the following is BEST to include in a business case when the return on investment (RIO)

for an information security is difficult to calculate? [43996]

A: Estimated increase in efficiency

B: Projected costs over time

C: Estimated reduction in risk

D: Projected increase in maturity level

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43996

97 Which of the following is the PRIMARY objective of reporting security metrics to stakeholders?

[43997]

A: To provide support for security audit activities

B: To identify key controls within the organization

C: To demonstrate alignment to the business strategy

D: To communicate the effectiveness of the security program

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43997

98 When recommending a preventive control against cross-site scripting in web applications, an

information security manager is MOST likely to suggest: [43998]

A: consolidating multiple sites into a single portal.

B: coding standards and code review.

C: using https in place of http.

D: hardening of the web server's operating system.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43998

99 Which of the following should be the FIRST step of incident response procedures? [43999]

A: Evaluate the cause of the control failure.

B: Perform a risk assessment to determine the business impact.

C: Identify if there is a need for additional technical assistance.

D: Classify the event depending on severity and type.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

43999

100 What should an information security manager do FIRST when a service provider that stores the

organization's confidential customer data experiences breach in its data center? [44000]

A: Engage an audit if the provider's data center.

B: Determine the impact of the breach.

C: Recommend canceling the outsourcing contract.

D: Apply remediation actions to counteract the breach.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

101 Which of the following is the MOST important consideration for designing an effective information

security governance framework? [44001]

A: Continuous audit cycle

B: Defined security metrics

C: Security policy provisions

D: Security controls automation

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44001

102 Which of the following devices, when placed in a demilitarized zone (DMZ), would be considered a

significant exposure? [44002]

A: Authentication server

B: Web server

C: Proxy server

D: Intrusion detection server

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44002

103 Which of the following is the MAIN concern when securing emerging technologies? [44003]

A: Compatibility with legacy systems

B: Unknown vulnerabilities

C: Integrating with existing access controls

D: Applying the corporate hardening standards

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44003

104 Risk identification, analysis and mitigation activities can BEST be integrated into business life cycle

processes by linking them to: [44004]

A: continuity planning.

B: compliance testing.

C: configuration management.

D: change management.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44004

105 During the establishment of a service level agreement (SLA) with a cloud service provider, it is

MOST important for the information security manager to: [44005]

A: set up proper communication paths with the provider.

B: update the security policy to reflect the provider's term of service.

C: understand the cloud storage architecture in use to determine security risk.

D: ensure security requirements are contractually enforceable.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

106 Which of the following is the BEST indication that an information security control is no longer

relevant? [44006]

A: Following the control costs the business more than not following it.

B: IT management does not support the control.

C: Users regularly bypass or ignore the control.

D: The control does not support a specific business function.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44006

107 An information security manager is evaluating the key risk indicators (KRIs) for an organization's

information security program. Which of the following would be the information security

manager's GREATEST concern? [44007]

A: Use of qualitative measures

B: Multiple KRIs for a single control process

C: Undefined thresholds to trigger alerts

D: Lack of formal KRI approval from IT management

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44007

108 An outsourced vendor handles an organization's business critical data. Which of the following is

the MOST effective way for the client organization to obtain assurance of the vendor's security

practices? [44008]

A: Reviewing the vendor's security audit reports

B: Requiring business continuity plans (BCPs) from the vendor

C: Verifying security certifications held by the vendor

D: Requiring periodic independent third-party reviews

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44008

109 When developing a new system, detailed information security functionality should FIRST be

addressed: [44009]

A: as part of prototyping.

B: during the system design phase.

C: when system requirements are defined.

D: as part of application development.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44009

110 Which of the following is the MOST relevant risk factor to an organization when employees use

social media? [44010]

A: Social media can be accessed from multiple locations.

B: Social media increases the velocity of risk and the threat capacity.

C: Social media offers a platform that can host cyber-attacks.

D: Social media can be used to gather intelligence for attacks.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

111 Which of the following is the MOST effective method to prevent a SQL injection in an employee

portal? [44011]

A: Conduct code reviews.

B: Enforce referential integrity on the database.

C: Reconfigure the database schema.

D: Conduct network penetration testing.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44011

112 When implementing a new risk assessment methodology, which of the following is the MOST

important requirement? [44012]

A: Risk assessments must be conducted by certified staff.

B: The methodology must be approved by the chief executive officer.

C: Risk assessments must be reviewed annually.

D: The methodology used must be consistent across the organization.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44012

113 Which of the following is the MOST important influence to the continued success of an

organization's information security strategy? [44013]

A: Information systems

B: Policy development

C: Organizational culture

D: Security processes

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44013

114 Which of the following is the MOST important reason for logging firewall activity? [44014]

A: Auditing purposes

B: Incident investigation

C: Firewall tuning

D: Intrusion detection

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44014

115 The PRIMARY focus of a training curriculum for members of an incident response team should be:

[44015]

A: technology training.

B: external corporate communication.

C: security awareness.

D: specific role training.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44015

116 An executive's personal mobile device used for business purposes is reported lost. The information

security manager should respond based on: [44016]

A: the business impact analysis (BIA).

B: incident classification.

C: asset management guidelines.

D: mobile device configuration.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44016

117 Which of the following is the BEST reason for delaying the application of a critical security patch?

[44017]

A: Conflicts with software development life cycle

B: Resource limitations

C: Lack of vulnerability management

D: Technology interdependences

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44017

118 When creating an information security governance program, which of the following will BEST

enable the organization to address regulatory compliance requirements? [44018]

A: Input from the security steering committee

B: A security control framework

C: An approved security strategy plan

D: Guidelines for processes and procedures

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44018

119 Which of the following is MOST important when prioritizing an information security incident?

[44019]

A: Organizational risk tolerance

B: Cost to contain and remediate the incident

C: Criticality of affected resources

D: Short-term impact to shareholder value

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44019

120 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 co [44020]

A: Determine a lower-cost approach to remediation.

B: Document and schedule a date to revisit the issue.

C: Shut down the business application.

D: Document and escalate to senior management.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

121 Exceptions to a security policy should be approved based PRIMARILY on: [44021]

A: risk appetite.

B: the external threat probability.

C: results of a business impact analysis (BIA).

D: the number of security incidents.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44021

122 Which of the following is MOST helpful for aligning security operations with the IT governance

framework? [44022]

A: Business impact analysis (BIA)

B: Security operations program

C: Security risk assessment

D: Information security policy

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44022

123 A third-party service provider is developing a mobile app for an organization's customers. Which of

the following issues should be of GREATEST concern to the information security management?

[44023]

A: Software escrow is not addressed in the contract.

B: The contract has no requirement for secure development practices.

C: The mobile app's programmers are all offshore contractors.

D: SLAs after deployment are not clearly defined.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44023

124 Following a highly sensitive data breach at a large company, all servers and workstations were

patched. The information security manager's NEXT step should be to: [44024]

A: inform senior management of changes in risk metrics.

B: perform an assessment to measure the current state.

C: deliver security awareness training.

D: ensure baseline back-ups are performed.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44024

125 The head of a department affected by a recent security incident expressed concern about not

being aware of the actions taken to resolve the incident. Which of the following is the BEST way to

address this issue? [44025]

A: Require management approval of the incident response plan.

B: Ensure better identification of incidents in the incident response plan.

C: Disseminate the incident response plan throughout the organization.

D: Discuss the definition of roles in the incident response plan.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44025

126 The MAIN reason for an information security manager to monitor industry level changes in the

business is to: [44026]

A: evaluate the effect of the changes on the levels of residual risk.

B: identify changes in the risk environment.

C: update information security policies in accordance with the changes.

D: change business objectives based on potential impact.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44026

127 When developing a protection strategy for outsourcing applications, the information security

manager MUST ensure that: [44027]

A: nondisclosure clauses are in the contract.

B: escrow agreements are in place.

C: the responsibility for security is transferred in the service level agreement (SLA).

D: the security requirements are included in the service level agreement (SLA).

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44027

128 Which of the following models provides a client organization with the MOST administrative control

over a cloud-hosted environment? [44028]

A: Infrastructure as a Service (IaaS)

B: Software as a Service (SaaS)

C: Storage as a Service (SaaS)

D: Platform as a Service (PaaS)

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44028

129 Which of the following should be an information security manager's FIRST course of action

following a decision to implement a new technology? [44029]

A: Perform a business impact analysis (BIA) on the new technology.

B: Determine security controls needed to support the new technology.

C: Perform a return-on-investment (ROI) analysis for the new technology.

D: Determine whether the new technology will comply with regulatory requirements.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44029

130 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: [44030]

A: evaluate the security policy and standards.

B: ensure compliance with international standards.

C: assess the ability to integrate the security department operations.

D: determine the security exposures.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44030

131 The PRIMARY goal of a post-incident review should be to [44031]

A: determine why the incident occurred.

B: determine how to improve the incident handling process.

C: establish the cost of the incident to the business.

D: identify policy changes to prevent a recurrence.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44031

132 An organization with a strict need-to-know information access policy is about to launch a

knowledge management intranet. Which of the following is the MOST important activity to ensure

compliance with existing security policies? [44032]

A: Develop a control procedure to check content before it is published.

B: Change organization policy to allow wider use of the new web site.

C: Ensure that access to the web site is limited to senior managers and the board.

D: Password-protect documents that contain confidential information.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44032

133 A data-hosting organization's data center houses servers, applications, and data for a large number

of geographically dispersed customers. Which of the following strategies would be the BEST

approach for developing a physical access control policy for th [44033]

A: Design single sign-on or federated access.

B: Conduct a risk assessment to determine security risks and mitigating controls.

C: Develop access control requirements for each system and application.

D: Review customers' security policies.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44033

134 The MAIN consideration when designing an incident escalation plan should be ensuring that:

[44034]

A: requirements cover forensic analysis.

B: information assets are classified.

C: appropriate stakeholders are involved.

D: high-impact risks have been identified.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44034

135 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? [44035]

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 corresponding controls are viewed as prohibitive to business operations.

D: The wording of the policy Is not tailored to the audience.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

136 A PRIMARY advantage of involving business management in evaluating and managing information

security risks is that they: [44036]

A: are more objective than security management.

B: better understand organizational risks.

C: better understand the security architecture.

D: can balance technical and business risks.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44036

137 When building a corporate-wide business continuity plan, it is discovered there are two separate

lines of business systems that could be impacted by the same threat. Which of the following is the

BEST method to determine the priority of system recovery i [44037]

A: Evaluating the cost associated with each system's outage

B: Reviewing the business plans of each department

C: Comparing the recovery point objectives (RPOs)

D: Reviewing each system's key performance indicators (KPIs)

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44037

138 What is the MOST effective way to ensure information security incidents will be managed

effectively and in a timely manner? [44038]

A: Establish and measure key performance indicators (KPIs).

B: Test incident response procedures regularly.

C: Communicate incident response procedures to staff.

D: Obtain senior management commitment.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44038

139 Which of the following is the BEST way to prevent recurrence of a security incident? [44039]

A: An expanded and more effective monitoring and detection process for incidents

B: Review and update security policy on a regular basis

C: Management support and approval of the incident response plan

D: An appropriate investigation into the root cause with corrective measures applied

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44039

140 Management is questioning the need for several items in the information security budget proposal.

Which of the following would have been MOST helpful prior to budget submission? [44040]

A: Benchmarking information security efforts of industry competitors

B: Obtaining better pricing from information security service vendors

C: Presenting a report of current threats to the organization

D: Educating management on information security best practices

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44040

141 Which of the following would BEST protect against web-based cross-domain attacks? [44041]

A: Network addressing scheme

B: Encryption controls

C: Application controls

D: Database hardening

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44041

142 Which of the following is the MOST important criterion for complete closure of a security incident?

[44042]

A: Level of potential impact

B: Root-cause analysis and lessons learned

C: Isolation and protection of affected resources

D: Reporting to senior management

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44042

143 When responding to an incident, which of the following is required to ensure evidence remains

legally admissible in court? [44043]

A: A documented incident response plan

B: Law enforcement oversight

C: Certified forensics examiners

D: Chain of custody

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44043

1. 144 Which of the following is the BEST course of action for an information security manager to align

security and business goals? [44044]

A: Conducting a business impact analysis (BIA)

B: Actively engaging with stakeholders

C: Reviewing the business strategy

D: Defining key performance indicators (KPIs)

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44044

145 The BEST way to ensure information security efforts and initiatives continue to support corporate

strategy is by: [44045]

A: including information security metrics in the organizational metrics.

B: conducting benchmarking with industry best practices.

C: including the CIO in the information security steering committee.

D: performing periodic internal audits of the information security program.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44045

146 Which of the following is the FIRST step required to achieve effective performance measurement?

[44046]

A: Implement control objectives.

B: Define meaningful metrics.

C: Validate and calibrate metrics.

D: Select and place sensors.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44046

147 Which of the following BEST ensures timely and reliable access to services? [44047]

A: Authenticity

B: Recovery time objective

C: Availability

D: Nonrepudiation

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44047

148 Which of the following is an indicator of improvement in the ability to identify security risks?

[44048]

A: Increased number of reported security incidents

B: Decreased number of staff requiring information security training

C: Increased number of security audit issues resolved

D: Decreased number of information security risk assessments

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44048

149 Which of the following is MOST important when establishing a successful information security

governance framework? [44049]

A: Identifying information security risk scenarios

B: Selecting information security steering committee members

C: Determining balanced scorecard metrics for information security

D: Developing an information security strategy

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44049

150 When facilitating the alignment of corporate governance and information security governance,

which of the following is the MOST important role of an organization's security steering

committee? [44050]

A: Obtaining support for the integration from business owners

B: Evaluating and reporting the degree of integration

C: Obtaining approval for the information security budget

D: Defining metrics to demonstrate alignment

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44050

151 Which of the following is the BEST way to determine if an organization's current risk level is within

the risk appetite? [44051]

A: Conducting a business impact analysis (BIA)

B: Implementing key risk indicators (KRIs)

C: Developing additional mitigating controls

D: Implementing key performance indicators (KPIs)

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44051

152 Which of the following is MOST relevant for an information security manager to communicate to IT

operations? [44052]

A: Vulnerability assessments

B: The level of exposure

C: The level of inherent risk

D: Threat assessments

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44052

153 Which of the following is MOST important for an information security manager to consider when

identifying information security resource requirements? [44053]

A: Current resourcing levels

B: Availability of potential resources

C: Information security strategy

D: Information security incidents

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44053

154 The MOST important reason to use a centralized mechanism to identify information security

incidents is to: [44054]

A: prevent unauthorized changes to networks.

B: detect threats across environments.

C: detect potential fraud.

D: comply with corporate policies.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44054

155 A risk has been formally accepted and documented. Which of the following is the MOST important

action for an information security manager? [44055]

A: Update risk tolerance levels.

B: Notify senior management and the board.

C: Monitor the environment for changes.

D: Re-evaluate the organization's risk appetite.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44055

156 Which of the following is the MOST important action when using a web application that has

recognized vulnerabilities? [44056]

A: Deploy an application firewall.

B: Deploy host-based intrusion detection.

C: Install anti-spyware software.

D: Monitor application level logs.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44056

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

process? [44057]

A: Assess the process according to information security policy

B: Benchmark the process against industry practices

C: Verify the use of a recognized control framework

D: Review the process for conformance with information security best practices

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44057

158 Which of the following BEST supports the alignment of information security with business

functions? [44058]

A: IT management support of security assessments

B: Business management participation in security penetration tests

C: Creation of a security steering committee

D: A focus on technology security risk within business processes

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44058

159 The BEST defense against phishing attempts within an organization is: [44059]

A: strengthening of firewall rules.

B: an intrusion detection system (IDS).

C: an intrusion prevention system (IPS).

D: filtering of e-mail.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44059

160 What should be an information security manager's PRIMARY objective in the event of a security

incident? [44060]

A: Ensure that normal operations are not disrupted

B: Contain the threat and restore operations in a timely manner

C: Identify the source of the breach and how it was perpetrated

D: Identify lapses in operational contol effectiveness

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44060

161 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? [44061]

A: Gap analysis results

B: Threat assessment results

C: Risk register

D: Risk heat map

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44061

162 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? [44062]

A: Determine the classification level of the information.

B: Seek business justification from the employee.

C: Block access to the cloud storage service.

D: Inform higher management of a security breach.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44062

163 The FIRST step in establishing an information security program is to: [44063]

A: define polices and standards that mitigate the organization's risks.

B: secure organizational commitment and support.

C: assess the organization's compliance with regulatory requirements.

D: determine the level of risk that is acceptable to some management.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44063

164 Which of the following is the MOST challenging aspect of securing Internet of Things (IoT) devices?

[44064]

A: Managing the diversity of IoT architecture

B: Training staff on IoT architecture

C: Evaluating the reputations of IoT vendors

D: Updating policies to include IoT devices

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44064

165 A CEO requests access to corporate documents from a mobile device that does not comply with

organizational policy. The information security manager should FIRST: [44065]

A: initiate an exception approval process

B: evaluate the business risk

C: deploy additional security controls

D: evaluate a third-party solution

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44065

166 When establishing classifications of security incidents for the development of an incident response

plan, which of the following provides the MOST valuable input? [44066]

A: The business continuity plan (BCP)

B: Vulnerability assessment results

C: Business impact analysis (BIA) results

D: Recommendations from senior management

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44066

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

consideration? [44067]

A: Risk matrices

B: Vulnerability scores

C: System criticalities

D: Threat profiles

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44067

168 Which of the following is the MOST effective way to ensure the process for granting access to new

employees is standardized and meets organizational security requirements? [44068]

A: Grant authorization to individual systems as required with the approval of information security

management

B: Adopt a standard template of access levels for all employees to be enacted upon hiring

C: Require managers of new hires be responsible for account setup and access during employee

orientation

D: Embed the authorization and creation of accounts with HR onboarding procedures

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44068

169 Which of the following would be MOST important to include in a bring your own device (BYOD)

policy with regard to lost or stolen devices? The need for employees to: [44069]

A: seek advice from the mobile service provider.

B: initiate the company's incident reporting process.

C: notify local law enforcement.

D: request a remote wipe of the device.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44069

170 Which of the following is the BEST advantage of a centralized information security organizational

structure? [44070]

A: It allows for a common level of assurance across the enterprise.

B: It is easier to manage and control business unit security teams.

C: It is more responsive to business unit needs.

D: It provides a faster turnaround for security waiver requests.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

171 Which of the following should be of GREATEST concern to an information security manager when

establishing a set of key risk indicators (KRIs)? [44071]

A: The organization has no historical data on previous security events.

B: Risk tolerance levels have not yet been established.

C: Several business functions have been outsourced to third-party vendors.

D: The impact of security risk on organizational objectives is not well understood.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44071

172 The PRIMARY reason for implementing scenario-based training for incident response is to : [44072]

A: verify threats and vulnerabilities faced by the incident response team

B: ensure staff knows where to report in the event evacuation is required

C: help incident response team members understand their assigned roles

D: assess the timeliness of the incident team response and remediation

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44072

173 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? [44073]

A: Change management

B: Access control management

C: Configuration management

D: Risk management

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44073

174 An organization has implemented a new customer relationship management (CRM) system. Who

should be responsible for enforcing authorized and controlled access to the CRM data? [44074]

A: The data owner

B: Internal IT audit

C: The data custodian

D: The information security manager

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44074

175 Which of the following outsourced services has the GREATEST need for security monitoring?

[44075]

A: Enterprise infrastructure

B: Application development

C: Virtual private network (VPN) services

D: Web site hosting

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44075

176 Which of the following is the MOST effective mitigation strategy to protect confidential

information from insider threats? [44076]

A: Defining segregation of duties

B: Performing an entitlement review process

C: Establishing authorization controls

D: Implementing authentication mechanisms

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44076

177 Management decisions concerning information security investments will be MOST effective when

they are based on: [44077]

A: an annual loss expectancy (ALE) determined from the history of security events.

B: the formalized acceptance of risk analysis by management.

C: the reporting of consistent and periodic assessments of risks.

D: a process for identifying and analyzing threats and vulnerabilities.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44077

178 Which of the following should be the PRIMARY consideration when developing a security

governance framework for an enterprise? [44078]

A: Results of a business impact analysis (BIA)

B: Assessment of the current security architecture

C: Understanding of the current business strategy

D: Benchmarking against industry best practice

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44078

179 When preventive controls to appropriately mitigate risk are not feasible, which of the following is

the MOST important action for the information security manager to perform? [44079]

A: Manage the impact.

B: Assess vulnerabilities.

C: Evaluate potential threats.

D: Identify unacceptable risk levels.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44079

180 Which of the following is the BEST way to sustain employee interest in information security

awareness in an organization? [44080]

A: Ensuring a common security awareness program for all staff

B: Relating security awareness programs to security policies

C: Ensuring all staff are involved

D: Using a variety of delivery methods

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44080

181 Application data integrity risk would be MOST directly addressed by a design that includes: [44081]

A: reconciliation routines such as checksums, hash totals, and record counts.

B: strict application of an authorized data dictionary.

C: access control technologies such as role-based entitlements.

D: application log requirements such as field-level audit trails and user activity logs.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44081

182 An organization was forced to pay a ransom to regain access to a critical database that had been

encrypted in a ransomware attack. What would have BEST prevented the need to make this

ransom payment? [44082]

A: Verifying the firewall is configured properly

B: Storing backups on a segregated network

C: Training employees on ransomware

D: Ensuring all changes are approved

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44082

183 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: [44083]

A: Create a comprehensive singular communication

B: Invoke the organization's incident response plan

C: Determine the needs and requirements of each audience

D: Set up communication channels for the target audience

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44083

184 A large organization is considering a policy that would allow employees to bring their own

smartphones into the organizational environment. The MOST important concern to the

information security manager should be the: [44084]

A: decrease in end user productivity.

B: impact on network capacity.

C: lack of a device management solution.

D: higher costs in supporting end users.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44084

185 Which of the following is the BEST approach to identify noncompliance issues with legal,

regulatory, and contractual requirements? [44085]

A: Risk assessment

B: Gap analysis

C: Vulnerability assessment

D: Business impact analysis (BIA)

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44085

186 An organization is concerned with the risk of information leakage caused by incorrect use of

personally owned smart devices by employees. What is the BEST way for the information security

manager to mitigate the associated risk? [44086]

A: Require employees to sign a nondisclosure agreement.

B: Implement a mobile device management solution.

C: implement a multi-factor authentication solution.

D: Document a bring-your-own-device (BYOD) policy.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44086

187 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? [44087]

A: Include information security criteria as part of vendor selection

B: Develop metrics for vendor performance

C: Include information security clauses in the vendor contract

D: Review third-party reports of potential vendors

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44087

188 Failure to include information security requirements within the build/buy decision would MOST

likely result in the need for: [44088]

A: commercial product compliance with corporate standards.

B: more stringent source programming standards.

C: compensating controls in the operational environment.

D: security scanning of operational platforms.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44088

189 Which of the following is MOST important when carrying out a forensic examination of a laptop to

determine an employee's involvement in a fraud? [44089]

A: The laptop should not be removed from the company premises

B: The investigation should be conducted on an image of the original disk drive

C: An HR representative should be present during the laptop examination

D: The employee's network access should be suspended

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44089

190 What should be the PRIMARY basis for establishing a recovery time objective (RTO) for a critical

business application? [44090]

A: Business impact analysis (BIA) results

B: Legal and regulatory requirements

C: Related business benchmarks

D: Risk assessment results

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

191 Segregation of duties is a security control PRIMARILY used to: [44091]

A: establish dual check.

B: establish hierarchy.

C: limit malicious behavior.

D: decentralize operations.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44091

192 Which of the following is the GREATEST risk of single sign-on? [44092]

A: Integration of single sign-on with the rest of the infrastructure is complicated.

B: It is a single point of failure for an enterprise access control process.

C: Password carelessness by one user may render the entire infrastructure vulnerable.

D: One administrator maintains the single sign-on solutions without segregation of duty.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44092

193 Without prior approval, a training department enrolled the company in a free cloud-based

collaboration site and invited employees to use it. Which of the following is the BEST response of

the information security manager? [44093]

A: Conduct a risk assessment and develop an impact analysis.

B: Update the risk register and review the information security strategy.

C: Report the activity to senior management.

D: Allow temporary use of the site and monitor for data leakage.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44093

194 Which of the following should cause the GREATEST concern for an information security manager

reviewing the effectiveness of an intrusion prevention system (IPS)? [44094]

A: Increase in false negatives

B: Decrease in malicious packets

C: Increase in crossover error rate

D: Decrease in false positives

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44094

195 Which of the following is the information security manager's PRIMARY role in the information

assets classification process? [44095]

A: Developing an asset classification model

B: Securing assets in accordance with their classification

C: Assigning asset ownership

D: Assigning the asset classification level

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44095

196 An organization's information security manager has learned that similar organizations have

become increasingly susceptible to spear phishing attacks. What is the BEST way to address this

concern? [44096]

A: Conduct a business impact analysis (BIA) of the threat

B: Include tips to identify threats in awareness training

C: Create a new security policy that staff must read and sign

D: Update data loss prevention (DLP) rules for email

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44096

197 An information security manager has been alerted to a possible incident involving a breach at one

of the organization's vendors. Which of the following should be done FIRST? [44097]

A: Engage the incident response team

B: Perform incident eradication

C: Perform incident recovery

D: Discontinue the relationship with the vendor

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44097

198 Which of the following will BEST provide an organization with ongoing assurance of the

information security services provided by a cloud provider? [44098]

A: Evaluating the provider's security incident response plan

B: Ensuring the provider's roles and responsibilities are established

C: Requiring periodic self-assessments by the provider

D: Continuous monitoring of information security risk profile

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44098

199 When designing an incident response plan to be agreed upon with a cloud computing vendor,

including which of the following will BEST help to ensure the effectiveness of the plan? [44099]

A: Responsibility and accountability assignments

B: Requirements for onsite recovery testing

C: An audit and compliance program

D: A training program for the vendor staff

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44099

200 An information security manager has identified and implemented mitigating controls according to

industry best practices. Which of the following is the GREATEST risk associated with this approach?

[44100]

A: The security program may not be aligned with organization objectives

B: The mitigation measures may not be updated in a timely manner

C: Important security controls may be missed without senior management input

D: The cost of control implementation may be too high

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44100

201 An organization's recent risk assessment has identified many areas of security risk, and senior

management has asked for a five-minute overview of the assessment results. Which of the

following is the information security manager's BEST option for present [44101]

A: Balanced scorecard

B: Risk register

C: Spider diagram

D: Risk heat map

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44101

202 What is the PRIMARY role of the information security program? [44102]

A: To deveolop and enforce a set of security policies aligned with the business

B: To educate stakeholders regarding information security requirements

C: To perform periodic risk assessments and business impact analysis (BIAs)

D: To provide guidance in managing organizational security risk

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44102

203 Which of the following metrics BEST evaluates the completeness of disaster recovery preparations?

[44103]

A: Ratio of successful to unsuccessful tests

B: Number of published application recovery plans

C: Ratio of recovery plan documents to total applications

D: Ratio of tested applications to total applications

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44103

204 In information security governance, the PRIMARY role of the board of directors is to ensure: [44104]

A: alignment with the strategic goals of the organization.

B: compliance with regulations and best practices.

C: approval of relevant policies and standards.

D: communication of security posture to stakeholders.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44104

205 Who should decide the extent to which an organization will comply with new cybersecurity

regulatory requirements? [44105]

A: Senior management

B: Information security manager

C: IT steering committee

D: Legal councel

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44105

206 Which of the following is MOST effective against system intrusions? [44106]

A: Continuous monitoring

B: Two-factor authentication

C: Layered protection

D: Penetration testing

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44106

207 Which of the following is the STRONGEST indicator of effective alignment between corporate

governance and information security governance? [44107]

A: Key performance indicators (KPIs) for controls trend positively

B: Senior management requests periodic information security updates

C: Information security initiatives meet scope, schedule, and budget

D: Senior management sponsors information security efforts

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44107

208 In addition to business alignment and security ownership, which of the following is MOST critical

for information security governance? [44108]

A: Auditability of systems

B: Compliance with policies

C: Reporting of security metrics

D: Executive sponsorship

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44108

209 The MOST important reason for an information security manager to be involved in the change

management process is to ensure that: [44109]

A: security controls drive technology changes

B: risks have been evaluated

C: security controls are updated regularly

D: potential vulnerabilities are identified

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44109

210 Which of the following would be the MOST important information to include in a business case for

an information security project in a highly regulated industry? [44110]

A: Compliance risk assessment

B: Critical audit findings

C: Industry comparison analysis

D: Number of reported security incidents

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44110

211 In an organization implementing a data classification program, ultimate responsibility for the data

on the database server lies with the: [44111]

A: database administrator.

B: information technology manager.

C: business unit manager.

D: information security manager.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44111

212 Which of the following MUST be established before implementing a data loss prevention (DLP)

system? [44112]

A: A data backup policy

B: A data recovery policy

C: Data classification

D: Privacy impact assessment

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44112

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

be included? [44113]

A: Explanation of information usage

B: Access control requirements

C: Limited liability clause

D: Information encryption requirements

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44113

214 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? [44114]

A: Monitor user activities on the network.

B: Publish the standards on the intranet landing page.

C: Establish an acceptable use policy.

D: Deploy a device management solution.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44114

215 To ensure adequate disaster-preparedness among IT infrastructure personnel, it is MOST

important to: [44115]

A: include end-user personnel in each recovery test

B: assign personnel-specific duties in the recovery plan

C: have the most experienced personnel participate in recovery tests

D: periodically rotate recovery-test participants

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44115

216 The MOST important reason that security risk assessments should be conducted frequently

throughout an organization is because: [44116]

A: threats to the organization may change.

B: compliance with legal and regulatory standards should be reassessed.

C: control effectiveness may weaken.

D: controls should be regularly tested.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44116

217 Which of the following would BEST enhance firewall security? [44117]

A: Placing the firewall on a screened subnet

B: Logging of security events

C: Implementing change control practices

D: Providing dynamic address assignment

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44117

218 Which of the following is the MOST important outcome of a well-implemented awareness

program? [44118]

A: Help desk response time to resolve incidents is improved

B: The number of successful social engineering attacks is reduced

C: The board is held accountable for risk management

D: The number of reported security incidents steadily decreases

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44118

219 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?

[44119]

A: Require remote wipe capabilities for devices.

B: Enforce passwords and data encryption on the devices.

C: Conduct security awareness training.

D: Review and update existing security policies.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44119

220 The PRIMARY goal of conducting a business impact analysis (BIA) as part of an overall continuity

planning process is to: [44120]

A: map the business process to supporting IT and other corporate resources

B: obtain the support of executive management

C: document the disaster recovery process

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

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44120

221 What should be an information security manager's FIRST course of action upon learning of a

security threat that has occurred in the industry for the first time? [44121]

A: Revise the organization's incident response plan

B: Update the relevant information security policy

C: Examine responses of victims that have been exposed to similar threats

D: Perform a control gap analysis of the organization's environment

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44121

222 Which of the following BEST describes a buffer overflow? [44122]

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

B: A program contains a hidden and unintended function that presents a security risk

C: A type of covert channel that captures data

D: Malicious code designed to interfere with normal operations

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44122

223 An organization has decided to implement a security information and event management (SIEM)

system. It is MOST important for the organization to consider: [44123]

A: industry best practices.

B: data ownership.

C: log sources.

D: threat assessments.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44123

224 The PRIMARY purpose of implementing information security governance metrics is to: [44124]

A: assess operational and program metrics

B: refine control operations

C: guide security towards the desired state

D: measure alignment with best practices

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44124

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

[44125]

A: Incident response time is improved.

B: The plan is enhanced to reflect the findings of the test.

C: The response includes escalation to senior management.

D: Test plan results are documented.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44125

226 Which of the following is the MOST effective method to help ensure information security incidents

are reported? [44126]

A: Implementing an incident management system

B: Providing information security awareness training to employees

C: Integrating information security language in corporate compliance rules

D: Integrating information security language in conditions of employment

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44126

227 Which of the following should be the PRIMARY consideration when selecting a recovery site?

[44127]

A: Recovery time objective

B: Recovery point objective

C: Geographical location

D: Regulatory requirements

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44127

228 When supporting an organization's privacy officer, which of the following is the information

security manager's PRIMARY role regarding primacy requirements? [44128]

A: Monitoring the transfer of private data

B: Conducting privacy awareness programs

C: Ensuring appropriate controls are in place

D: Determining data classification

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44128

229 Penetration testing is MOST appropriate when a: [44129]

A: new system is being designed.

B: security incident has occurred.

C: security policy is being developed.

D: new system is about to go live.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44129

230 Which of the following is the BEST performed by the security department? [44130]

A: Approving standards for accessing the operating system

B: Logging unauthorized access to the operating system

C: Managing user profiles for accessing the operating system

D: Provisioning users to access the operating system

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44130

231 When customer data has been compromised, an organization should contact law enforcement

authorities: [44131]

A: if the attack comes from an international source.

B: when directed by the information security manager.

C: if there is potential impact to the organization.

D: in accordance with the corporate communication policy.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44131

232 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? [44132]

A: Calculate security implementation costs

B: Review cloud provider independent assessment reports

C: Provide cloud security requirements

D: Evaluate service level agreements (SLAs)

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44132

233 Which of the following is the MOST important prerequisite to performing an information security

risk assessment? [44133]

A: Classifying assets

B: Reviewing the business impact analysis (BIA)

C: Assessing threats and vulnerabilities

D: Determining risk tolerance

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44133

234 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? [44134]

A: Auditing the service delivery of third-party providers

B: Requiring third parties to sign confidentiality agreements

C: Providing information security training to third-party personnel

D: Including information security clauses within contracts

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44134

235 An information security program should be established PRIMARILY on the basis of: [44135]

A: the approved information security strategy.

B: the approved risk management approach.

C: data security regulatory requirements.

D: senior management input.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44135

236 Which of the following is the PRIMARY reason for performing an analysis of the threat landscape

on a regular basis? [44136]

A: To determine if existing business continuity plans are adequate

B: To determine the basis for proposing an increase in security budgets

C: To determine if existing vulnerabilities present a risk

D: To determine critical information for executive management

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44136

237 Which of the following would provide senior management with the BEST information to better

understand the organization's information security risk profile? [44137]

A: Scenarios that impact business operations

B: Scenarios that disrupt client services

C: Scenarios that impact business goals

D: Scenarios that have a monetary impact

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44137

238 Which of the following should be the FIRST step to ensure system updates are applied in a timely

manner? [44138]

A: Create a regression test plan to ensure business operation is not interrupted

B: Run a patch management scan to discover which patches are missing from each machine

C: Cross-reference all missing patches to establish the date each patch was introduced

D: Establish a risk-based assessment process for prioritizing patch implementation

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44138

239 An organization is considering whether to allow employees to use personal computing devices for

business purposes. To BEST facilitate senior management's decision, the information security

manager should: [44139]

A: conduct a risk assessment.

B: develop a business case.

C: map the strategy to business objectives.

D: perform a cost-benefit analysis.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44139

240 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? [44140]

A: Design mitigating controls for the exceptions

B: Inform respective risk owners of the impact of exceptions

C: Report the noncompliance to the board of directors

D: Prioritize the risk and implement treatment options

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44140

241 A business unit uses e-commerce with a strong password policy. Many customers complain that

they cannot remember their password because they are too long and complex. The business unit

states it is imperative to improve the customer experience. The inf [44141]

A: Change the password policy to improve the customer experience.

B: Research alternative secure methods of identity verification.

C: Recommend implementing two-factor authentication.

D: Evaluate the impact of the customer's experience on business revenue.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44141

242 Which of the following is the BEST mechanism to prevent data loss in the event personal

computing equipment is stolen or lost? [44142]

A: Data encryption

B: Remote access to device

C: Presonal firewall

D: Data leakage prevention (DLP)

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44142

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

[44143]

A: Password composition requirements

B: Consequences of noncompliance

C: Audit trail review requirements

D: Security monitoring strategy

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44143

244 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 important action

of the information security manager? [44144]

A: Follow the outsourcer's response plan.

B: Alert the appropriate law enforcement authorities.

C: Refer to the organization's response plan.

D: Notify the outsourcer of the privacy breach.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44144

245 Which of the following provides the MOST comprehensive understanding of an organization's

information security posture? [44145]

A: The organization's security incident trends

B: Risk management metrics

C: Results of vulnerability assessments

D: External audit findings

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44145

246 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? [44146]

A: Assess the security risk associated with the use of social networks

B: Develop security controls for the use of social networks

C: Establish processes to publish content on social networks

D: Conduct vulnerability assessments on social network platforms

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44146

247 Which of the following is the BEST evidence that an organization's information security governance

framework is effective? [44147]

A: Threats to the organization have diminished

B: The risk register is reviewed annually

C: The framework focuses primarily on technical controls

D: The framework can adapt to organizational changes

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44147

248 Deciding the level of protection a particular asset should be given is BEST determined by: [44148]

A: a risk analysis.

B: a threat assessment.

C: a vulnerability assessment.

D: corporate risk appetite.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44148

249 Which of the following is MOST effective in the strategic alignment of security initiatives? [44149]

A: Key information security policy are updated on a regular basis.

B: Policies are created with input from business unit managers.

C: Business leaders participate in information security decision making.

D: A security steering committee is set up within the IT deployment.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44149

250 Mitigating technology risks to acceptable levels should be based PRIMARILY upon: [44150]

A: business process reengineering.

B: business process requirements.

C: legal and regulatory requirements.

D: information security budget.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44150

251 Which of the following is MOST important for an information security manager to communicate to

senior management regarding the security program? [44151]

A: Impact analysts results

B: User roles and responsibilities

C: Security architecture changes

D: Potential risks and exposures

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44151

252 Using which of the following metrics will BEST help to determine the resiliency of IT infrastructure

security controls? [44152]

A: Number of successful disaster recovery tests

B: Frequency of updates to system software

C: Number of incidents resulting in disruptions

D: Percentage of outstanding high-risk audit issues

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44152

253 Which of the following enables compliance with a nonrepudiation policy requirement for electronic

transactions? [44153]

A: Digital signatures

B: One-time passwords

C: Encrypted passwords

D: Digital certificates

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44153

254 Following a successful and well-publicized hacking incident, an organization aligns plans to improve

application security. Which of the following is a security project risk? [44154]

A: Critical evidence may be lost.

B: The reputation of the organization may be damaged.

C: A trapdoor may have been installed in the application.

D: Resources may not be available to support the implementation.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44154

255 What should an information security team do FIRST when notified by the help desk that an

employee's computer has been infected with malware? [44155]

A: Isolate the computer from the network

B: Use anti-malware software to clean the infected computer

C: Restore the files from a secure backup

D: Take a forensic copy of the hard drive

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44155

256 When multiple Internet intrusions on a server are detected, the PRIMARY concern of the

information security manager should be to ensure that the: [44156]

A: server is backed up to the network

B: integrity of evidence is preserved

C: forensic investigation software is loaded on the server

D: server is unplugged from power

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44156

257 Which of the following needs to be established between an IT service provider and its clients to

BEST enable adequate continuity of service in preparation for an outage? [44157]

A: Reciprocal site agreement

B: Server maintenance plans

C: Recovery time objectives (RTOs)

D: Data retention policies

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44157

258 Which of the following would be MOST helpful to the information security manager tasked with

enforcing enhanced password standards? [44158]

A: Conducting password strength testing

B: Reeducating end users on creating strong complex passwords

C: Implementing a centralized identity management system

D: Implementing technical password controls to include strong complexity

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44158

259 What is the PRIMARY benefit to executive management when audit, risk, and security functions are

aligned? [44159]

A: More timely risk reporting

B: Reduced number of assurance reports

C: More effective decision making

D: More efficient incident handling

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44159

260 The PRIMARY objective of a risk response strategy should be: [44160]

A: threat reduction.

B: regulatory compliance.

C: senior management buy-in.

D: appropriate control selection.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44160

261 Which of the following is the MOST important factor to consider when establishing a severity

hierarchy for information security incidents? [44161]

A: Regulatory compliance

B: Management support

C: Business impact

D: Residual risk

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44161

262 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?

[44162]

A: Availability of current infrastructure documentation

B: Capability to take a snapshot of virtual machines

C: Availability of web application firewall logs

D: Capability of online virtual machine analysis

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44162

263 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? [44163]

A: Implement additional controls.

B: Report to senior management.

C: Initiate incident response processes.

D: Conduct an impact analysis.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44163

264 Following a malicious security incident, an organization has decided to prosecute those

responsible. Which of the following will BEST facilitate the forensic investigation? [44164]

A: Identifying the affected environment

B: Performing a backup of affected systems

C: Determining the degree of loss

D: Maintaining chain of custody

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44164

265 Which of the following provides the GREATEST assurance that an organization allocates

appropriate resources to respond to information security events? [44165]

A: Information security policies and standards

B: Threat analysis and intelligence reports

C: Incident classification procedures

D: An approved IT staffing plan

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

266 An information security steering group should: [44166]

A: provide general oversight and guidance.

B: develop information security policies.

C: establish information security baselines.

D: oversee the daily operations of the security program.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44166

267 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? [44167]

A: Review the provider's information security policies and procedures

B: Obtain documentation of the encryption management practices

C: Verify the provider follows a cloud service framework standard

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

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44167

268 Which of the following metrics is the BEST indicator of an abuse of the change management

process that could compromise information security? [44168]

A: Percentage of changes that include post-approval supplemental add-ons

B: Large percentage decrease in monthly change requests

C: High ratio of lines of code changed to total lines of code

D: Small number of change requests

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44168

269 A payroll application system accepts individual user sign-on IDs and then connects to its database

using a single application ID. The GREATEST weakness under this system architecture is that:

[44169]

A: the database becomes unavailable if the password of the application ID expires.

B: an incident involving unauthorized access to data cannot be tied to a specific user.

C: users can gain direct access to the application ID and circumvent data controls.

D: when multiple sessions with the same application ID collide, the database locks up.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44169

270 Which of the following should be of GREATEST concern to a newly hired information security

manager regarding security compliance? [44170]

A: Lack of standard operating procedures

B: Lack of risk assessments

C: Lack of executive support

D: Lack of security audits

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44170

271 An information security manager is preparing an incident response plan. Which of the following is

the MOST important consideration when responding to an incident involving sensitive customer

data? [44171]

A: The assignment of a forensics team

B: Following defined post-incident review procedures

C: The ability to recover from the incident in a timely manner

D: The ability to obtain incident information in a timely manner

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44171

272 Which of the following is MOST important to consider when handling digital evidence during the

forensics investigation of a cybercrime? [44172]

A: Global standards

B: Industry best practices

C: Business strategies

D: Local regulations

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44172

273 Which of the following processes would BEST aid an information security manager in resolving

systemic security issues? [44173]

A: Business impact analysis (BIA)

B: Security reviews

C: Reinforced security controls

D: Root cause analysis

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44173

274 Which of the following is the MOST effective method for categorizing system and data criticality

during the risk assessment process? [44174]

A: Interview the asset owners

B: Interview data custodians

C: Interview senior management

D: Interview members of the board

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44174

275 Which of the following will BEST enable an effective information asset classification process?

[44175]

A: Including security requirements in the classification process

B: Analyzing audit findings

C: Assigning ownership

D: Reviewing the recovery time objective (RTO) requirements of the asset

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44175

276 Which of the following is the MOST significant security risk in IT asset management? [44176]

A: IT assets may be used by staff for private purposes.

B: Unregistered IT assets may not be supported.

C: Unregistered IT assets may not be included in security documentation.

D: Unregistered IT assets may not be configured properly.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44176

277 Which of the following should be the FIRST step to ensure an information security program meets

the requirements of new regulations? [44177]

A: Conduct a gap analysis to determine necessary changes

B: Validate the asset classification schema

C: Assess organizational security controls

D: Integrate compliance into the risk management process

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44177

278 An organization has announced new initiatives to establish a big data platform and develop mobile

apps. What is the FIRST step when defining new human resource requirements? [44178]

A: Determine the security technology requirements for the initiatives.

B: Analyze the skills necessary to support the new initiatives.

C: Request additional funding for recruiting and training.

D: Benchmark to an industry peer.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44178

279 Which of the following statements indicates that a previously failing security program is becoming

successful? [44179]

A: Management's attention and budget are now focused on risk reduction.

B: More employees and stakeholders are attending security awareness programs.

C: The number of threats has been reduced.

D: The number of vulnerability false positives is decreasing.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44179

280 Which of the following is an important criterion for developing effective key risk indicators (KRIs) to

monitor information security risk? [44180]

A: The indicator should align with key performance indicators (KPIs) and measure root causes of

process performance issues.

B: The indicator should possess a high correlation with a specific risk and be measured on a regular

basis.

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

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

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44180

281 When preparing a strategy for protection from SQL injection attacks, it is MOST important for the

information security manager to involve: [44181]

A: the security operations center

B: business owners

C: application developers

D: senior management

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44181

282 Which of the following BEST enables a more efficient incident reporting process? [44182]

A: Training end users to identify abnormal events

B: Educating the incident response team on escalation procedures

C: Training executive management for communication with external entities

D: Educating IT teams on compliance requirements

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44182

283 Which of the following would be MOST helpful in gaining support for a business case for an

information security initiative? [44183]

A: Presenting a solution comparison matrix

B: Emphasizing threats to the organization

C: Demonstrating organizational alignment

D: Referencing control deficiencies

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44183

284 An information security manager learns of a new international standard related to information

security. Which of the following would be the BEST course of action? [44184]

A: Review industry peers responses to the new standard.

B: Consult with legal counsel on the standard's applicability to regulations.

C: Determine whether the organization can benefit from adopting the new standard.

D: Perform a gap analysis between the new standard and existing practices.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44184

285 An organization's information security manager is performing a post-incident review of a security

incident in which the following events occurred:  1. A bad actor broke into a business-critical FTP

server by brute forcing an administrative password 2. The [44185]

A: Potential access to the administrator console

B: Disclosure of stolen data

C: Removal of data

D: Downtime of the service

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44185

286 Which of the following is MOST critical for responding effectively to security breaches? [44186]

A: Management communication

B: Counterattack techniques

C: Evidence gathering

D: Root cause analysis

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44186

287 Which of the following is the MOST important component of a risk profile? [44187]

A: Data classification results

B: Penetration test results

C: Risk assessment methodology

D: Risk management framework

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44187

288 An information security manager has discovered a potential security breach in a server that

supports a critical business process. Which of the following should be the information security

manager's FIRST course of action? [44188]

A: Shut down the server in an organized manner

B: Notify the business process owner

C: Validate that there has been an incident

D: Inform senior management of the incident

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44188

289 Which of the following should be done FIRST when handling multiple confirmed incidents raised at

the same time? [44189]

A: Inform senior management

B: Categorize incidents by the value of the affected asset

C: Activate the business continuity plan (BCP)

D: Update the business impact assessment

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44189

290 Which of the following would be MOST useful in a report to senior management for evaluating

changes in the organization's information security risk position? [44190]

A: Trend analysis

B: Industry benchmarks

C: Management action plan

D: Risk register

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44190

291 From a business perspective the MOST important function of information security is to support:

[44191]

A: predictable operations.

B: international standards.

C: security awareness.

D: corporate policy.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44191

292 Cold sites for disaster recovery events are MOST helpful in situations in which a company: [44192]

A: has a limited budget for coverage

B: does not require any telecommunications connectivity

C: is located in close proximity to the cold site

D: uses highly specialized equipment that must be custom manufactured

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44192

293 Which of the following is the BEST reason to initiate a reassessment of current risk? [44193]

A: Follow-up to an audit report

B: A recent security incident

C: Certification requirements

D: Changes to security personnel

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44193

294 Which of the following security characteristics is MOST important to the protection of customer

data in an online transaction system? [44194]

A: Data segregation

B: Availability

C: Audit monitoring

D: Authentication

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44194

295 Which of the following will BEST facilitate the understanding of information security responsibilities

by users across the organization? [44195]

A: Conducting security awareness training with performance incentives

B: Communicating security responsibilities as an acceptable usage policy

C: Warning users that disciplinary action will be taken for violations

D: Incorporating information security into the organization's code of conduct

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44195

296 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? [44196]

A: Control owner responses based on a root cause analysis

B: An accountability risk to initiate remediation activities

C: A plan for mitigating the risk due to noncompliance

D: The impact of noncompliance on the organization's risk profile

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44196

297 The MOST likely reason to use qualitative security risk assessments instead of quantitative

methods is when: [44197]

A: available data is too subjective

B: a security program requires independent expression of risks

C: an organization provides services instead of hard goods

D: a mature security program is in place

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44197

298 Which of the following BEST demonstrates the maturity of an information security monitoring

program? [44198]

A: Senior management regularly reviews security standards

B: Information security key risk indicators (KRIs) are tied to business operations

C: The information security program was introduced with a thorough business case

D: Risk scenarios are regularly entered into a risk register

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44198

299 Which of the following is the BEST way for an organization that outsources many business

processes to gain assurance that services provided are adequately secured? [44199]

A: Review the service providers' information security policies and procedures

B: Conduct regular vulnerability assessments on the service providers' IT systems

C: Perform regular audits on the service providers' applicable controls

D: Provide information security awareness training to service provider staff

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44199

300 Which of the following sites would be MOST appropriate in the case of a very short recovery time

objective (RTO)? [44200]

A: Redundant

B: Shared

C: Warm

D: Mobile

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44200

301 A new version of an information security regulation is published that requires an organization's

compliance. The information security manager should FIRST: [44201]

A: perform an audit based on the new version of the regulation.

B: conduct a risk assessment to determine the risk of noncompliance.

C: conduct benchmarking against similar organizations.

D: perform a gap analysis against the new regulation.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44201

302 Adding security requirements late in the software development life cycle (SDLC) would most likely

result in: [44202]

A: operational efficiency

B: compensating controls

C: cost savings

D: clearer understanding of requirements

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44202

303 Who is MOST important to include when establishing the response process for a significant security

breach that would impact the IT infrastructure and cause customer data loss? [44203]

A: An independent auditor for identification of control deficiencies

B: A penetration tester to validate the attack

C: A forensics expert for evidence management

D: A damage assessment expert for calculating losses

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44203

304 When an operating system is being hardened, it is MOST important for an information security

manager to ensure that [44204]

A: system logs are activated.

B: default passwords are changed.

C: anonymous access is removed.

D: file access is restricted.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44204

305 The MOST important outcome of information security governance is: [44205]

A: business risk avoidance.

B: informed decision making.

C: alignment with business goals.

D: alignment with compliance requirements.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44205

306 Information security governance is PRIMARILY a: [44206]

A: process issue

B: people issue

C: business issue

D: regulatory issue

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44206

307 Which of the following best enables effective closure of noncompliance issues? [44207]

A: Insuring against the risk

B: Capturing issues in a risk register

C: Executing an approved security governance framewo mitigation plan

D: Performing control self-assessments (CSAs)

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44207

308 Which of the following is the MOST effective way of ensuring that business units comply with an

information rk? [44208]

A: Conducting a business impact analysis (BIA)

B: Conducting information security awareness training

C: Integrating security requirements with processes

D: Performing security assessments and gap analyses

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44208

309 Senior management has just accepted the risk of noncompliance with a new regulation. What

should the information security manager do NEXT? [44209]

A: Update details within the risk register.

B: Reassess the organization's risk tolerance.

C: Report the decision to the compliance officer.

D: Assess the impact of the regulation.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44209

310 The effectiveness of security awareness programs in fostering positive security cultures is most

dependent upon employee: [44210]

A: awareness of regulatory requirements

B: ability to carry out security-related procedures

C: understanding of the penalties for noncompliance

D: ownership of security responsibilities

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44210

311 An information security manager has been asked to create a strategy to protect the organization's

information from a variety of threat vectors. Which of the following should be done FIRST? [44211]

A: Perform a threat modeling exercise.

B: Develop a risk profile.

C: Design risk management processes.

D: Select a governance framework.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44211

312 Which of the following is the PRIMARY advantage of having an established information security

governance framework in place when an organization is adopting emerging technologies? [44212]

A: A cost-benefit analysis process would be easier to perform.

B: An emerging technologies strategy would be in place.

C: End-user acceptance of emerging technologies has been established.

D: An effective security risk management process is established.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44212

313 The primary objective for using threat modeling in web application development should be to:

[44213]

A: develop application development standards

B: determine if penetration testing is necessary

C: build security into the design

D: review application source code

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44213

314 Of the following, who should have PRIMARY responsibility for assessing the security risk associated

with an outsourced cloud provider contract? [44214]

A: Chief information officer

B: Service delivery manager

C: Compliance manager

D: Information security manager

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44214

315 Which of the following should be an information security manager's MOST important

consideration when conducting a physical security review of a potential outsourced data center?

[44215]

A: Environmental factors of the surrounding location

B: Availability of network circuit connections

C: Distance of the data center from the corporate office

D: Proximity to law enforcement

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44215

316 Which of the following will identify a deviation in the information security management process

from generally accepted standards of good practices? [44216]

A: Gap analysis

B: Penetration resting

C: Risk assessment

D: Business impact analysis (BIA)

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44216

317 Which of the following should be an information security manager's FIRST course of action if

notified by a third party that the organization's client data is being sold online? [44217]

A: Validate whether the information is accurate.

B: Shut down the applications that contain the client data.

C: Report the incident to senior management.

D: Determine how the client data was compromised.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44217

318 During a review to approve a penetration test plan, which of the following should be an

information security manager's PRIMARY concern? [44218]

A: Penetration test team's deviation from scope

B: Unauthorized access to administrative utilities

C: False positive alarms to operations staff

D: Impact on production systems

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44218

319 Which of the following would MOST likely require a business continuity plan to be invoked? [44219]

A: An unauthorized visitor discovered in the data center

B: A distributed denial of service attack on an email server

C: An epidemic preventing staff from performing job functions

D: A hacker holding personally identifiable information hostage

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44219

320 Which of the following would provide the MOST comprehensive view of the effectiveness of the

information security function within an organization? [44220]

A: An incident reporting system

B: Examples of compliance with security processes

C: A balanced scorecard

D: An interview with senior managers

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44220

321 Business applications should be selected for disaster recovery testing on the basis of: [44221]

A: recovery time objectives (RTOs).

B: the results of contingency desktop checks.

C: criticality to the enterprise.

D: the number of failure that are being tested.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44221

322 What information is MOST helpful in demonstrating to senior management how information

security governance aligns with business objectives? [44222]

A: Updates on information security projects in development

B: Drafts of proposed policy changes

C: Metrics of key information security deliverables

D: A list of monitored threats, risks, and exposures

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44222

323 Information security governance is PRIMARILY driven by which of the following? [44223]

A: Regulatory requirements

B: Litigation potential

C: Business strategy

D: Technology constraints

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44223

324 Several significant risks have been identified after a centralized risk register was compiled and

prioritized. The information security manager's MOST important action is to: [44224]

A: provide senior management with risk treatment options.

B: design and implement controls to reduce the risk.

C: consult external third parties on how to treat the risk.

D: ensure that employees are aware of the risk.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44224

325 Which of the following is the MOST important reason to consider the role of the IT service desk

when developing incident handling procedures? [44225]

A: The service desk provides a source for the identification of security incidents.

B: Service desk personnel have information on how to resolve common systems issues.

C: The service desk provides information to prioritize systems recovery based on user demand.

D: Untrained service desk personnel may be a cause of security incidents.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44225

326 Which of the following stakeholders would provide the BEST guidance in aligning the information

security strategy with organizational goals? [44226]

A: Information security steering committee

B: Chief information officer (CIO)

C: Chief information security officer (CISO)

D: Board of directors

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44226

327 Within the confidentiality, integrity, and availability (CIA) triad, which of the following activities

BEST supports the concept of integrity? [44227]

A: Utilizing a formal change management process

B: Enforcing service level agreements (SLAs)

C: Implementing a data classification schema

D: Ensuring encryption for data in transit

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44227

328 Which of the following is MOST important for the effectiveness of an incident response function?

[44228]

A: Automated incident tracking and reporting tools

B: Enterprise security management system and forensic tools

C: Training of all users on when and how to report

D: Establishing prior contacts with law enforcement

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44228

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

program? [44229]

A: Reduction in the cost of risk remediation for an organization

B: Reduction in the number of threats to an organization

C: Reduction in the number of vulnerabilities in an organization

D: Reduction in the amount of risk exposure in an organization

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44229

330 Key systems necessary for branch operations reside at corporate headquarters. Branch A is

negotiating with a third party to provide disaster recovery facilities. Which of the following

contract terms would be the MOST significant concern? [44230]

A: The hot site for the branch may have to be shared.

B: Connectivity is not provided from the hot site to corporate headquarters.

C: Penalty clauses for nonperformance are not included in contract.

D: The right to audit the hot site is not provided in the contract.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

331 An organization is developing a disaster recovery plan for a data center that hosts multiple

applications. The application recovery sequence would BEST be determined through an analysis

of: [44231]

A: Recovery point objectives (RPOs).

B: The data classification scheme.

C: Recovery time objectives (RTOs).

D: Key performance indicators (KPIs).

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44231

332 Which type of test is MOST effective in communicating the roles of end users to support timely

identification and response to information security incidents? [44232]

A: Simulation

B: Walk-through

C: Parallel

D: Complete failover

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44232

333 Which of the following should be reviewed to obtain a structured overview of relevant information

about an information security investment? [44233]

A: Quantitative risk analysis report

B: Security balanced scorecard

C: Business case

D: Information security strategy

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44233

334 Which of the following will BEST ensure that risk is evaluated on system level changes? [44234]

A: Security should be integrated in the change control process.

B: Implement a centralized change management system.

C: Senior management must sign-off on changes.

D: System development staff receives regular security training.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44234

335 When supporting a large corporation's board of directors in the development of governance, which

of the following is the PRIMARY function of the information security manager? [44235]

A: Gaining commitment of senior management

B: Preparing the security budget

C: Providing advice and guidance

D: Developing a balanced scorecard

A 4

$$1 CIS Information Security 2: 3:

336 A newly hired information security manager for a small organization has been tasked with

improving data security. The BEST way to understand the organization's security posture would be

to: [44236]

A: perform a gap analysis based on industry best practices.

B: review previous vulnerabilities.

C: identify and classify business processes.

D: engage a third party to perform a security assessment.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44236

337 Which of the following is the best way to ensure the effectiveness of a role-based access scheme?

[44237]

A: Review the number of unauthorized access attempts.

B: Implement centralized event logging.

C: Review the number of exceptions granted.

D: Implement a self-service password system.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44237

338 Calculation of the recovery time objective (RTO) is necessary to determine the: [44238]

A: annual loss expectancy (ALE).

B: priority of restoration.

C: time required to restore files.

D: point of synchronization.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44238

339 An organization has a policy in which all criminal activity is prosecuted. What is MOST important

for the information security manager to ensure when an employee is suspected of using a

company computer to commit fraud? [44239]

A: The forensics process is immediately initiated.

B: The incident response plan is initiated.

C: The employee's log files are backed up.

D: Senior management is informed of the situation.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44239

340 Which of the following is the MOST effective way to achieve the integration of information security

governance into corporate governance? [44240]

A: Ensure information security aligns with IT strategy.

B: Ensure information security efforts support business goals.

C: Align information security budget requests to organizational goals.

D: Provide periodic IT balanced scorecards to senior management.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44240

341 Which of the following is the BEST way to align security and business strategies? [44241]

A: Include security risk as part of corporate risk management.

B: Integrate information security governance into corporate governance.

C: Establish key performance indicators (KPIs) for business through security processes.

D: Develop a balanced scorecard for security.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44241

342 A team developing an interface to a key financial system has identified a security flaw in one of the

libraries. Remediating the flaw would require major system redesign. What should the information

security manager do NEXT? [44242]

A: Conduct a comprehensive source code review.

B: Instruct the development team to remediate the flaw.

C: Confirm the impact with the business owner.

D: Hire a consultant to design proper remediation controls.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44242

343 An application system stores customer confidential data and encryption is not practical. The best

measure to protect against data disclosure is: [44243]

A: single sign-on

B: multi-factor access controls

C: nondisclosure agreements (NDA)

D: regular review of access logs

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44243

344 Which of the following elements of risk is MOST difficult to quantify? [44244]

A: Vulnerabilities

B: Countermeasures

C: Asset values

D: Threats

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44244

345 Which of the following is MOST helpful in protecting against hacking attempts on the production

network? [44245]

A: Intrusion prevention systems

B: Security information and even management (SEM) tools

C: Network penetration testing

D: Decentralized honeypot networks

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44245

346 A risk analysis for a new system is being performed. For which of the following is business

knowledge MORE important than IT knowledge? [44246]

A: Vulnerability analysis

B: Balanced scorecard

C: Cost-benefit analysis

D: Impact analysis

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44246

347 When developing security standards, which of the following would be MOST appropriate to

include? [44247]

A: Accountability for licenses

B: Acceptable use of IT assets

C: Operating system requirements

D: Inventory management

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44247

348 Which of the following should be done FIRST when implementing policies to address an upcoming

new data privacy regulation? [44248]

A: Segregate system processing personal data from other systems on the network.

B: Understand what technologies are required for personal data protection.

C: Prohibit further collection of personal data until the regulation is implemented.

D: Understand which types of personal data are covered by the new regulation.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44248

349 Which of the following is the GREATEST risk to consider when a rival organization purchases a

business unit within an organization? [44249]

A: Senior business management will not understand technical risks.

B: The business unit's confidential information will be transferred to the rival organization during

the separation.

C: Loss of corporate knowledge.

D: Access and permissions to the corporate network from the business until remain after the sale.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44249

350 An organization's senior management wants to allow employees to access an internal application

using their personal mobile devices. Which of the following should be the information security

managers FIRST course of action? [44250]

A: Develop a personal device policy

B: Conduct security testing

C: Require device encryption

D: Assess the security risk

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

351 A risk profile supports effective security decisions PRIMARILY because it: [44251]

A: defines how to best mitigate future risks.

B: identifies priorities for risk reduction.

C: enables comparison with industry best practices.

D: describes security threats.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44251

352 After logging in to a web application, additional authentication is required at various application

points. Which of the following is the PRIMARY reason for such an approach? [44252]

A: To ensure access rights meet classification requirements

B: To support strong two-factor authentication protocols

C: To implement a challenge response test

D: To meet single sign-on authentication standards

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44252

353 An information security manager learns that the root password of an external FTP server may be

subject to brute force attacks. Which of the following would be the MOST appropriate way to

reduce the likelihood of a successful attack? [44253]

A: Block the source IP address of the attacker.

B: Lock remote logon after multiple failed attempts.

C: Disable access to the externally facing server.

D: Install an intrusion detection system (IDS).

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44253

354 Which of the following is the BEST criterion to use when classifying assets? [44254]

A: The market value of the assets

B: Annual loss expectancy (ALE)

C: Value of the assets relative to the organization

D: Recovery time objective (RTO)

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44254

355 For proper escalation of events, it is MOST important for the information security manager to

ensure: [44255]

A: incident severity levels are defined.

B: the incident team is adequately staffed.

C: the incident response plan is approved.

D: incident documentation templates are created.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44255

356 Which of the following is MOST likely to reduce the effectiveness of a signature-based intrusion

detection system (IDS)? [44256]

A: The activities being monitored deviate from what is considered normal.

B: The information regarding monitored activities becomes stale.

C: The pattern of normal behavior changes quickly and dramatically.

D: The environment is complex.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44256

357 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? [44257]

A: Implement remote wipe capability.

B: Create an acceptable use policy.

C: Deploy mobile device management (MDM).

D: Conduct a mobile device risk assessment.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44257

358 An information security manager is preparing a presentation to obtain support for a security

initiative. Which of the following would be the BEST way to obtain management's commitment for

the initiative? [44258]

A: Include historical data of reported incidents.

B: Provide the estimated return on investment.

C: Provide an analysis of current risk exposures.

D: Include industry benchmarking comparisons.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44258

359 A new organization has been hit with a ransomware attack that is critically impacting its business

operations. The organization does not yet have a proper incident response plan, but it does have a

backup procedure for restoration of data. Which of the fo [44259]

A: Recommend that management pay the ransom.

B: Establish an incident response plan.

C: Contact the legal department.

D: Isolate the affected system.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44259

360 When developing an incident response plan, the information security manager should: [44260]

A: include response scenarios that have been approved previously by business management.

B: determine recovery time objectives (RTOs).

C: allow IT to decide which systems can be removed from the infrastructure.

D: require IT to invoke the business continuity plan.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44260

361 Which of the following would BEST help to ensure an organization's information security manager

strategy is aligned with business objectives? [44261]

A: Implementing an automated solution for monitoring information security processes

B: Requesting senior management to periodically review security incidents

C: Establishing metrics to measure the effectiveness of the information security program

D: Establishing a change control updating of security policies.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44261

362 A hacking group has posted an organization's employee data on social media. What should the

information security manager do FIRST? [44262]

A: Notify law enforcement.

B: Initiate the incident response process.

C: Inform the impacted employees.

D: Review system audit logs.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44262

363 Which of the following would be the BEST way for a company to reduce the risk of data loss

resulting from employee-owned devices accessing the corporate email system? [44263]

A: Link the bring-your-own-device (BYOD) policy to the existing staff disciplinary policy.

B: Require employees to undergo training before permitting access to the corporate email service.

C: Require employees to install a reputable mobile anti-virus solution on their personal devices.

D: Use a mobile device management solution (MDM) to isolate the local corporate email storage.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44263

364 When information security management is receiving an increased number of false positive incident

reports, which of the following is MOST important to review? [44264]

A: The security awareness programs

B: Firewall logs

C: The risk management processes

D: Post-incident analysis results

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44264

365 Which of the following provide the BEST means of ensuring business units outside of IT have their

information security concerns addressed? [44265]

A: Inclusion of business unit management in the information security steering committee

B: A comprehensive list of business processes performed by each business unit

C: Targeted user security awareness programs for business units outside of IT

D: Involvement of senior management in information security policy development

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44265

366 When defining responsibilities with a cloud computing vendor, which of the following should be

regarded as a shared responsibility between user and provider? [44266]

A: Data ownership

B: Access log review

C: Application logging

D: Incident response

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44266

367 Which of the following would be MOST helpful to reduce the amount of time needed by an

incident response team to determine appropriate actions? [44267]

A: Rehearsing incident response procedures, roles and responsibilities

B: Providing annual awareness training regarding incident response for team members

C: Validating the incident response plan against industry best practices

D: Defining incident severity levels during a business impact analysis (BIA)

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44267

368 An information security manager that is utilizing a public cloud is performing a root cause

investigation of an incident that took place in that environment. Which of the following should be

the security manager's MAIN concern? [44268]

A: Limited access to information

B: Shared infrastructure with other subscribers

C: Transaction records split into multiple cloud locations

D: Lack of security log filtering

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44268

369 A security incident has resulted in a failure of the enterprise resource planning (ERP) system. While

the incident is handled by the incident response team, the help desk is overrun by queries from

department managers on the state of the ERP system. What [44269]

A: Lack of knowledgeable help desk staff

B: An inadequate business impact analysis (BIA)

C: An inadequate communication plan

D: Lack of organization-wide security awareness

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44269

370 An organization is considering moving one of its critical business applications to a cloud hosting

service. The cloud provider may not provide the same level of security for this application as the

organization. Which of the following will provide the B [44270]

A: Risk assessment

B: Vulnerability assessment

C: Risk governance framework

D: Cloud security strategy

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

371 Senior management has allocated funding to each of the organization's divisions to address

information security vulnerabilities. The funding is based on each division's technology budget

from the previous fiscal year. Which of the following should be of [44271]

A: Redundant controls may be implemented across divisions.

B: Information security governance could be decentralized by division.

C: Areas of highest risk may not be adequately prioritized for treatment.

D: Return on investment may be inconsistently reported to senior management.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44271

372 An information security manager has researched several options for handling ongoing security

concerns and will be presenting these solutions to business managers. Which of the following will

BEST enable business managers to make an informed decision? [44272]

A: Business impact analysis (BIA)

B: Cost-benefit analysis

C: Risk analysis

D: Gap analysis

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44272

373 Which of the following should be the PRIMARY consideration for an information security manager

when designing security controls for a newly acquired business application? [44273]

A: The IT security architecture framework

B: Known vulnerabilities in the application

C: Business processes supported by the application

D: Cost-benefit analysis of current controls

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44273

374 Which is the MOST important driver for effectively communicating the progress of a new

information security program's implementation to key stakeholders? [44274]

A: Understanding stakeholder needs that influence program objectives

B: Facilitating stakeholder understanding of program-related technology concepts

C: Documenting risk that could impact achievement of program objectives

D: Designing universal key performance indicators (KPIs) for the program

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44274

375 An internal audit has found that critical patches were not implemented within the timeline

established by policy without a valid reason. Which of the following is the BEST course of action to

address the audit findings? [44275]

A: Evaluate patch management training.

B: Monitor and notify IT staff of critical patches.

C: Perform regular audits on the implementation of critical patches.

D: Assess the patch management process.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44275

376 Which is MOST important when contracting an external party to perform a penetration test?

[44276]

A: Define the project scope.

B: Increase the frequency of log reviews.

C: Provide network documentation.

D: Obtain approval from IT management.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44276

377 Ensuring that an organization can conduct security reviews within third-party facilities is PRIMARILY

enabled by: [44277]

A: service level agreements (SLAs)

B: acceptance of the organization's security policies

C: contractual agreements

D: audit guidelines

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44277

378 To implement a security framework, an information security manager must FIRST develop: [44278]

A: security standards.

B: security procedures.

C: a security policy.

D: security guidelines.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44278

379 The BEST way to determine the current state of information security with regard to defined

security objectives is by performing a: [44279]

A: risk assessment.

B: gap analysis.

C: cost-benefit analysis.

D: business impact analysis (BIA).

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44279

380 Which of the following should be the PRIMARY input when defining the desired state of security

within an organization? [44280]

A: Acceptable risk level

B: Annual loss expectancy

C: External audit results

D: Level of business impact

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44280

381 An information security manager has implemented an ongoing security awareness training

program. Employee participation has been decreasing over the year, while the number of malware

and phishing incidents from email has been increasing. What is the inform [44281]

A: Include regular phishing campaigns after each training session.

B: Make the training program mandatory and enforce sanctions for noncompliance.

C: Report the findings to senior management with recommendations.

D: Perform a risk assessment and share results with employees.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44281

382 An organization is considering a self-service solution for the deployment of virtualized

development servers. Which of the following should be the information security manager's

PRIMARY concern? [44282]

A: Ability to maintain server security baseline

B: Segregation of servers from the production environment

C: Generation of excessive security event logs

D: Ability to remain current with patches

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44282

383 Which of the following is the MOST critical security risk to consider for a start-up company in an

emerging field? [44283]

A: Disclosure of financial statements

B: Loss of intellectual property

C: A lack of security policies and procedures

D: New entries into the emerging marketplace

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44283

384 When training an incident response team, the advantage of using tabletop exercises is that they:

[44284]

A: enable the team to develop effective response interactions.

B: ensure that the team can respond to any incident.

C: provide the team with practical experience in responding to incidents.

D: remove the need to involve senior managers in the response process.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44284

385 Threat and vulnerability assessments are important PRIMARILY because they are: [44285]

A: needed to estimate risk

B: the basis for setting control objectives

C: elements of the organization's security posture

D: used to establish security investments

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44285

386 The value of information assets relative to the organization is best determined by: [44286]

A: a threat assessment

B: an asset classification

C: an impact analysis

D: a risk assessment

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44286

387 Which of the following is the BEST method to determine whether an information security program

meets an organization's business objectives? [44287]

A: Implement performance measures.

B: Perform a business impact analysis (BIA).

C: Review against international security standards.

D: Conduct an annual enterprise-wide security evaluation.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44287

388 Which of the following has the PRIMARY responsibility of ensuring an organization's information

security strategy supports business goals? [44288]

A: Audit committee

B: Information security steering committee

C: Chief executive officer (CEO)

D: Chief information security officer (CISO)

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44288

389 A business unit manager wants to adopt an emerging technology that may affect the organization.

Which of the following would be the information security manager's BEST course of action? [44289]

A: Perform a business impact analysis (BIA)

B: Review the business case

C: Review vendor documentation

D: Perform a threat analysis

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44289

390 Which of the following is the MOST effective control to reduce the impact of ransomware attacks?

[44290]

A: Backup strategy

B: Antivirus software

C: Intrusion detection system (IDS)

D: Security awareness training

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44290

391 An organization with a maturing incident response program conducts post-incident reviews for all

major information security incidents. The PRIMARY goal of these reviews should be to: [44291]

A: prepare properly vetted notifications regarding the incidents to external parties.

B: identify who should be held accountable for the security incidents.

C: document and report the root cause of the incidents for senior management.

D: identify security program gaps or systemic weaknesses that need correction.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44291

392 Which of the following BEST describes an intrusion detection system (IDS) that learns the system

behaviors prior to detecting potential intrusions? [44292]

A: Host-based IDS

B: Anomaly-based IDS

C: Network-based IDS

D: Application-based IDS

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44292

393 Information security policies should be designed PRIMRY on the basis of: [44293]

A: business risks.

B: business demands.

C: international standards.

D: inherent risks.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44293

394 The PRIMARY role of an information security steering group is to ensure that: [44294]

A: security policies address business issues.

B: security procedures and practice are in line with formal policies.

C: there is compliance with software e-copyright legislation.

D: there is compliance with security standards.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44294

395 Which of the following is MOST relevant for an information security manager to communicate to

the board of directors? [44295]

A: The level of inherent risk

B: Threat assessments

C: Vulnerability assessments

D: The level of exposure

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44295

396 Which of the following circumstances would MOST likely require and update to an organization's

information security incident response plan? [44296]

A: A new business application has been implemented.

B: A new business strategy has been developed.

C: A high-risk vulnerability has been detected.

D: The organizational structure has changed.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44296

397 The PRIMARY purpose of a periodic threat and risk assessment report to senior management is to

communicate the: [44297]

A: probability of future incidents.

B: status of the security posture.

C: risk acceptance criteria.

D: cost-benefit of security controls.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44297

398 Which of the following is the BEST way to demonstrate to senior management that organizational

security practices comply with industry standards? [44298]

A: Existence of an industry-accepted framework

B: Up-to-date policy and procedures documentation

C: A report on the maturity of controls

D: Results of an independent assessment

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44298

399 What should be the information security manager's MOST important consideration when planning

a disaster recovery test? [44299]

A: Organization-wide involvement

B: Documented escalation processes

C: Impact to production systems

D: Stakeholder notification procedures

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44299

400 An organization's marketing department has requested access to cloud-based collaboration sites

for exchanging media files with external marketing companies. As a result, the information

security manager has been asked to perform a risk assessment. Which [44300]

A: Methods for transferring the information

B: The security of the third-party cloud provider

C: Reputation of the external marketing companies

D: The information to be exchanged

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

401 Which of the following is an example of a vulnerability? [44301]

A: Defective software

B: Natural disasters

C: Unauthorized users

D: Ransomware

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44301

402 An information security manager is asked to provide evidence that the organization is fulfilling its

legal obligation to protect personally identifiable information (PII). Which of the following would

be [44302]

A: Metrics related to program effectiveness

B: Written policies and standards

C: Privacy awareness training

D: Risk assessments of privacy-related applications

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44302

403 Which of the following is the PRIMARY objective of incident classification? [44303]

A: Increasing response efficiency

B: Enabling incident reporting

C: Complying with regulatory requirements

D: Reducing escalations to management

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44303

404 When establishing the trigger levels for an organization's key risk indicators (KRIs), the thresholds

should be based primarily on the organization's: [44304]

A: risk register

B: current threat level

C: risk response capability

D: risk appetite

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44304

405 An internal control audit has revealed a control deficiency related to a legacy system where the

compensating controls no longer appear to be effective. Which of the following would BEST help

the information security manager determine the security requir [44305]

A: Risk assessment

B: Gap analysis

C: Cost-benefit analysis

D: Business case

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44305

406 For an organization with operations in different parts of the world, the BEST approach for ensuring

that security policies do not conflict with local laws and regulations is to: [44306]

A: refer to an external global standard to avoid any regional conflict.

B: adopt uniform policies.

C: make policies at a sufficiently high level, so they are globally applicable.

D: establish a hierarchy of global and local policies.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44306

407 The PRIMARY purpose of aligning information security with corporate governance objectives is to:

[44307]

A: identify an organization's tolerance for risk.

B: re-align roles and responsibilities.

C: build capabilities to improve security processes.

D: consistently manage significant areas of risk.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44307

408 Which of the following is the PRIMARY benefit of using agentless endpoint security solutions?

[44308]

A: More comprehensive information results

B: Decreased administration

C: Increased resiliency

D: Decreased network bandwidth usage

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44308

409 Which of the following is the PRIMARY purpose for establishing a bring your own device (BYOD)

policy permits application downloads from designated online markets, stores, or repositories?

[44309]

A: Enhance IT application support for users.

B: Protect against malware-based attacks.

C: Allow IT to monitor application usage.

D: Conserve storage for approved applications.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44309

410 The frequency of conducting business impact analysis (BIA) should primarily be based on: [44310]

A: business continuity plan (BCP) testing

B: changes in regulatory requirements

C: changes in business processes

D: the number of security incidents

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44310

411 An organization's IT department is undertaking a large virtualization project to reduce its physical

server footprint. Which of the following should be the highest priority of the information security

manager? [44311]

A: Selecting the virtualization software

B: Determining how incidents will be managed

C: Being involved at the design stage of the project

D: Ensuring the project has appropriate security funding

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44311

412 Which of the following is the KEY outcome of conducting a post-incident review? [44312]

A: Root cause is validated.

B: Chain of custody is maintained.

C: Risk appetite is validated.

D: Compliance requirements are met.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44312

413 Which of the following is MOST important for an information security manager to highlight when

presenting the organization's security posture to an executive audience? [44313]

A: Performance metrics specific to business unit security awareness training

B: The number of emails blocked by the data loss prevention (DlP) system

C: Security risks that may inhibit business objectives

D: Published sophisticated security threats targeting the industry

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44313

414 Which of the following is the MOST important outcome of senior management's analysis of

information security metrics? [44314]

A: The integration of information security with corporate governance

B: The establishment of a risk acceptance process

C: The alignment of the information security budget to corporate funding

D: The alignment of security and IT objectives

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44314

415 Which of the following is the MOST significant benefit of effective change management? [44315]

A: Information security management is involved with the change advisory board

B: Release management is considered in the process

C: Security implications are considered as a standard practice

D: All provisioned modifications are approved by information security

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44315

416 The MOST important objective of monitoring key risk indicators (KRIs) related to information

security is to: [44316]

A: minimize loss from security incidents.

B: identify change in security exposures.

C: reduce risk management costs.

D: meet regulatory compliance requirements.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44316

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

first consideration? [44317]

A: Data isolation

B: Data backup

C: Data transfer

D: Data classification

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44317

418 Establishing which of the following is the BEST way of ensuring that the emergence of new risk is

promptly identified? [44318]

A: Regular risk reporting

B: Risk monitoring processes

C: Change control procedures

D: Incident monitoring activities

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44318

419 Which of the following would BEST support a business case to implement a data leakage

prevention (DLP) solution? [44319]

A: An unusual upward trend in outbound email volume

B: Industry benchmark of DLP investments

C: A risk assessment on the threat of data leakage

D: Lack of visibility into previous data leakage incidents

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44319

420 Which of the following presents the greatest concern to the information security manager when

using account locking features on an online application? It can increase vulnerability to: [44320]

A: social engineering

B: phishing

C: denial of service

D: brute force attacks

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44320

421 Which of the following should be the MOST important consideration when implementing an

information security framework? [44321]

A: Risk appetite

B: Audit findings

C: Compliance requirements

D: Technical capabilities

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44321

422 An information security manager is developing evidence preservation procedures for an incident

response plan. Which of the following would be the BEST source of guidance for requirements

associated with the procedures? [44322]

A: Legal counsel

B: Executive management

C: Data owners

D: IT management

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44322

423 Which of the following is the BEST way to identify the potential impact of a successful attack on an

organization's mission critical applications? [44323]

A: Conduct penetration testing.

B: Execute regular vulnerability scans.

C: Perform an application vulnerability review.

D: Perform an independent code review.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44323

424 Which of the following is the responsibility of a data owner? [44324]

A: Investigating and resolving suspicious database activity

B: Testing to determine whether the data can be recovered successfully

C: Maintaining the integrity of the database

D: Classifying the data in accordance with security policy

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44324

425 Which of the following is BEST determined by using technical metrics? [44325]

A: Whether security resources are adequately allocated

B: How well the security strategy is aligned with organizational objectives

C: Whether controls are operating effectively

D: How well security risk is being managed

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44325

426 Risk reporting requirements should be PRIMARILY based on: [44326]

A: criteria approved by management

B: policies approved by information security

C: events defined by information security

D: the criticality of assets

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44326

427 An information security manager is implementing controls to protect the organization's data. The

FIRST step in this process should be to: [44327]

A: implement access controls

B: classify the data

C: encrypt the data

D: monitor access to the data

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44327

428 Which of the following is the PRIMARY purpose of data classification? [44328]

A: To provide a basis for protecting data

B: To ensure integrity of data

C: To determine access rights to data

D: To select encryption technology

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44328

429 Which of the following BEST demonstrates effective information security management within an

organization? [44329]

A: Employees support decisions made by infromation security management.

B: Information security governance is incorporated into organizational governance.

C: Control ownership is assigned to parties who can accept loses related to control failure.

D: Excessive risk exposure in one department can be absorbed by other departments

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44329

430 Which of the following is the BEST way to determine if an information security program aligns with

corporate governance? [44330]

A: Evaluate funding for security initiatives.

B: Survey end users about corporate governance.

C: Review information security policies.

D: Review the balanced scorecard.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44330

431 Which of the following is MOST important to have in place to help secure ongoing funding for the

information security program? [44331]

A: Information security risk register

B: Information security strategy

C: Threat assessment report

D: Security Balanced Scorecard

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44331

432 During the restoration of several servers, a critical process that services external customers was

restored late due to a failure, resulting in lost revenue. Which of the following would have BEST

help to prevent this occurrence? [44332]

A: Validation of senior management's risk tolerance

B: Updates to the business impact analysis (BIA)

C: More effective disaster recovery plan (DRP) testing

D: Improvements to incident identification methods

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44332

433 Which of the following is most important for an information security manager to regularly report

to senior management? [44333]

A: Results of penetration tests

B: Impact of untreated risks

C: Threat analysis reports

D: Audit reports

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44333

434 A risk assessment report shows that phishing attacks are an emerging threat for an organization

that supports online financial services. Which of the following is the information security manager's

BEST course of action? [44334]

A: Update antivirus software

B: Implement spam protection

C: Conduct corporate awareness training

D: Transfer risk with insurance coverage

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44334

435 Conducting a cost-benefit analysis for a security investment is important because it [44335]

A: supports asset classification.

B: quantifies return on security investment.

C: supports justification for expenditure.

D: quantifies residual risk.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44335

436 Which of the following is the BEST approach when using sensitive customer data during the testing

phase of a systems development project? [44336]

A: Establish the test environment on a separate network.

B: Monitor the test environment for data loss.

C: Implement equivalent controls to those on the source system.

D: Sanitize customer data.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44336

437 Planning for the implementation of an information security program is MOST effective when it:

[44337]

A: uses decision trees to prioritize security projects.

B: applies gap analysis to current and future business plans.

C: applies technology-driven solutions to identified needs.

D: uses risk-based analysis for security projects.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44337

438 Which of the following metrics would BEST determine the effectiveness of an application security

testing program? [44338]

A: Average time to release code into production

B: Number of security defects discovered in development versus production

C: Average time to fix each discovered security defect

D: Number of detected security defects per thousand lines of code

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44338

439 Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?

[44339]

A: Risk assessment

B: Business impact analysis (BIA)

C: Asset classification

D: Business process mapping

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44339

440 Shortly after installation, an intrusion detection system (IDS) reports a violation. Which of the

following is the MOST likely explanation? [44340]

A: The violation is a false positive.

B: A routine IDS signature file download has occurred.

C: A routine IDS log file upload has occurred.

D: An intrusion has occurred.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44340

441 In risk assessment, after the identification of threats to organizational assets, the information

security manager would: [44341]

A: evaluate the controls currently in place.

B: implement controls to achieve target risk levels.

C: request funding for the security program.

D: determine threats to be reported to upper management.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44341

442 An organization's information security manager will find it most difficult to perform a post-incidnet

review of a data leakage event when it is related to: [44342]

A: private cloud services

B: corporate mobile devices

C: outsourced service providers

D: public cloud services

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44342

443 During a new user provisioning process, who should have PRIMARY responsibility for determining

appropriate access levels? [44343]

A: System owner

B: IT service manager

C: Security staff

D: Human resource manager

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44343

444 Which of the following is the MOST important factor when determining the frequency of

information security risk reassessment? [44344]

A: Risk priority

B: Risk metrics

C: Mitigating controls

D: Audit findings

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44344

445 Which of the following approaches is BEST for selecting controls to minimize information security

risks? [44345]

A: Cost-benefit analysis

B: Control-effectiveness

C: Risk assessment

D: Industry best practices

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44345

446 The risk of mishandling alerts identified by an intrusion detection system (IDS) would be the

GREATEST when: [44346]

A: operations and monitoring are handled by different teams.

B: The IT infrastructure is diverse.

C: IDS sensors are misconfigured.

D: standard operating procedures are not formalized.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44346

447 An incident was detected where customer records were altered without authorization. The

GREATEST concern for forensic analysis would be that the log data: [44347]

A: has been disclosed.

B: could be temporarily available.

C: may not be time-synchronized.

D: may be modified.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44347

448 Which of the following would provide the BEST justification for a new information security

investment? [44348]

A: Defined key performance indicators (KPIs)

B: Senior management involvement in project prioritization

C: Projected reduction in risk

D: Results of a comprehensive threat analysis

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44348

449 Web application firewalls are needed in addition to other intrusion prevention and detection

technology primarily because: [44349]

A: they recognize web application protocols

B: they prevent modification of application source code

C: web services require unique forensic evidence

D: web services are prone to attacks

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44349

450 The BEST way to minimize errors in the response to an incident is to: [44350]

A: follow standard operating procedures.

B: analyze the situation during the incident.

C: implement vendor recommendations.

D: reference system administration manuals.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44350

451 Which of the following is most important for an information security manager to consider when

developing a new information security policy? [44351]

A: Organizational goals and objectives

B: Alignment with industry standards

C: Organizational culture and complexity

D: Information security budget allocation

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44351

452 Which of the following is the best evidence that information security governance works as a

business enabler? [44352]

A: Business initiatives are within risk tolerance

B: Business initiatives are prioritized over security initiatives

C: Security initiatives have positive return on investment (ROI)

D: Security key performance indicators (KPIs) are included in management briefings

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44352

453 Which of the following is the best way to provide management with meaningful information

regarding the performance of the information security program against strategic objectives?

[44353]

A: Issue periodic reports to demonstrate compliance with security standards

B: Develop an information security heat map

C: Publish the information security strategy across the organization

D: Establish a balanced scorecard dashboard

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44353

454 In which of the following situations is it most important to escalate an incident response to senior

management? [44354]

A: The time-related service levels for response are below risk threshold levels

B: The impact of the incident exceeds the organization's risk tolerance

C: The owner of the affected business function is not available

D: The incident impacts a business-critical system

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44354

455 Which of the following is the first step to promoting acceptable behavior with regard to

information security throughout an organization? [44355]

A: Automate controls that enforce acceptable use

B: Required signed acknowledgment of acceptable use policies

C: Conduct targeted acceptable use training for management and staff

D: Incorporate information security standards into performance evaluations

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44355

456 Which of the following practices best supports the achievement of information security program

objectives in the IT function? [44356]

A: Continuous security auditing of IT service processes

B: IT management sign-off on information security policies

C: Review and approval of IT projects by the information security manager

D: Participation of IT stakeholders in the security program steering committee

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44356

457 The integration of information security risk management processes within corporate risk

management processes will most likely result in: [44357]

A: information security controls that reduce enterprise risk

B: improved efficiencies of security operations

C: more effective security risk management processes

D: senior management approval of the information security budgets

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44357

458 Which of the following should an information security manager do first when an organization plans

to migrate all internally hosted applications to the cloud? [44358]

A: Access the risk associated with the cloud services

B: Determine information security requirements for the cloud

C: Develop key risk indicators (KPIs)

D: Create an information security action plan

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44358

459 A business unit has updated its long-term business plan to include a strategy of upgrading

information management systems to increase productivity. To support this initiative, what should

be the primary basis for updating the corresponding information sec [44359]

A: The information security framework

B: IT risk assessment results

C: The IT strategy

D: The business strategy

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44359

460 A new mobile application is unable to adhere to the organization's authentication policy. Which of

the following would be the information security manager's best course of action? [44360]

A: Investigate alternative mobile applications

B: Accept the risk and document the exception

C: Determine alternative controls

D: Modify the policy to accommodate the application capabilities

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44360

461 Which of the following should the information security manager do first after a security incident

has been reported? [44361]

A: Determine the degree of loss resulting from the incident

B: Identify the scope and size of the affected environment

C: Identify the possible source of attack

D: Retrieve the information needed to confirm the incident

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44361

462 A recent phishing attack investigation showed that several employees had used their work email

addresses to create personal accounts on a shopping site that had been breached. What is the best

way to prevent this behavior in the future? [44362]

A: Send periodic fake phishing emails to employees and track responses

B: Update the incident response plan to address this situation

C: Conduct information security awareness training for employees

D: Block personal shopping sites using proxy filtering

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44362

463 Which of the following is the primary product of a business impact analysis (BIA)? [44363]

A: Well-defined incident escalation procedures

B: A heat map of business risk scenarios

C: Prioritization of vulnerabilities for remediation

D: Prioritization of assets for business recovery

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44363

464 Which of the following is the greatest benefit of a comprehensive set of security program metrics?

[44364]

A: Validation of risk assessment results

B: Visibility to security compliance

C: Data to support risk assessments

D: Evaluation of the security strategy

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44364

465 The primary purpose of a risk assessment is to enable business leaders to: [44365]

A: define key risk indicators (KRIs)

B: align information security to business objectives

C: manage information security expenditures

D: make informed decisions

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44365

466 Which of the following is the best indication of an effective information security program? [44366]

A: Key risk indicators (KPIs) are established

B: Risk is treated to an acceptable level

C: Policies are approved by senior management

D: Policies and standards are developed

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44366

467 Which of the following is primarily influenced by a business impact analysis (BIA)? [44367]

A: Security strategy

B: IT strategy

C: Risk mitigation strategy

D: Recovery strategy

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44367

468 Which of the following is an information security manager's best course of action upon

identification of a shadow IT application being used by a business unit? [44368]

A: Perform a vendor due diligence review

B: Report the application to the IT department

C: Determine the nature of information within the application

D: Notify senior management of the application

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44368

469 An organization uses a particular encryption protocol for externally facing web pages and key

financial services. A security firm publicizes a critical security flaw in the encryption protocol. Which

of the following should the information security manage [44369]

A: Remediate the vulnerability

B: Perform a risk assessment

C: Isolate potentially vulnerable systems

D: Activate the incident response team

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44369

470 Which of the following is the BEST way to rigorously test a disaster recovery plan for a mission-

critical system without disrupting business operations? [44370]

A: Checklist review

B: Structed walk-through

C: Parallel testing

D: Simulation testing

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44370

471 Which of the following is MOST important when establishing effective information security

metrics? [44371]

A: Mapping each metric to a specific control

B: Receiving senior management approval

C: Mapping each metric to information security objectives

D: Understanding the business objectives

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44371

472 Which of the following is MOST important for an information security manager to include in a

report to senior management following a post-incident review? [44372]

A: Detailed metrics

B: The incident response plan

C: Lessons learned

D: Snapshot of system logs

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44372

473 Which of the following is the MOST effective way to ensure the information security risk associated

with third-party services is addressed? [44373]

A: Include appropriate security requirements in the contract.

B: Perform a risk assessment on the services.

C: Conduct a security test of the services prior to implementation.

D: Provide security awareness training to third-party employees.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44373

474 Which of the following BEST indicates that information security will be considered when new IT

technologies are implemented across an organization? [44374]

A: Employees receive information security awareness training.

B: The information security manager is on the IT architecture review board.

C: IT employee job descriptions include information security roles and responsibilities.

D: The information security function reports to the chief information officer.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44374

475 Which of the following provides the BEST preparation for handling the breach of a corporate web

site? [44375]

A: Review of cyber liability insurance coverage

B: Incident response testing

C: Documented data recovery procedures

D: Web server penetration testing

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44375

476 Which of the following is the MOST important outcome of monitoring and reporting on

information security processes? [44376]

A: Ensuring information security operations support control objectives

B: Ensuring information security operations meet service level agreements (SLA)

C: Ensuring information security operations are reviewed for effectiveness

D: Ensuring information security operations follow approved procedures

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44376

477 Which of the following is the BEST way to prevent segregation of duties violations? [44377]

A: Enable data encryption with strong keys.

B: Review access log for violations.

C: Implement role-based access.

D: Implement an identify management system.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44377

478 An organization has experienced a ransomware attack. Which of the following is the BEST course of

action to prevent further attacks? [44378]

A: Implement application whitelisting.

B: Implement application blacklisting.

C: Refuse to pay the ransom.

D: Update the security policy.

B 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44378

479 The FIRST step in developing a business case is to: [44379]

A: determine the probability of success.

B: calculate the return on investment.

C: analyze the cost-effectiveness.

D: define the issues to be addressed.

D 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44379

480 Which of the following is the PRIMARY benefit of using a tabletop method to conduct an incident

response exercise? [44380]

A: Visibility into personnel effectiveness is increased.

B: The impact of IT systems on business operations is quantified.

C: Potential impact to business operations is minimized.

D: The readiness of applications for testing is ensured.

C 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44380

481 The MOST appropriate role for senior management in supporting information security is the:

[44381]

A: evaluation of vendors offering security products.

B: assessment of risks to the organization.

C: approval of policy statements and funding.

D: monitoring adherence to regulatory requirements.

C 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44381

482 The MAIN goal of an information security strategic plan is to: [44382]

A: develop a risk assessment plan.

B: develop a data protection plan.

C: protect information assets and resources.

D: establish security governance.

C 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44382

483 The PRIMARY goal of developing an information security strategy is to: [44383]

A: establish security metrics and performance monitoring.

B: educate business process owners regarding their duties.

C: ensure that legal and regulatory requirements are met

D: support the business objectives of the organization.

D 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44383

484 When an information security manager is developing a strategic plan for information security, the

timeline for the plan should be: [44384]

A: aligned with the IT strategic plan.

B: based on the current rate of technological change.

C: three-to-five years for both hardware and software.

D: aligned with the business strategy.

D 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44384

485 An organization's information security strategy should be based on: [44385]

A: managing risk relative to business objectives.

B: managing risk to a zero level and minimizing insurance premiums.

C: avoiding occurrence of risks so that insurance is not required.

D: transferring most risks to insurers and saving on control costs.

A 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44385

486 When implementing effective security governance within the requirements of the company's

security strategy, which of the following is the MOST important factor to consider? [44386]

A: Preserving the confidentiality of sensitive data

B: Establishing international security standards for data sharing

C: Adhering to corporate privacy standards

D: Establishing system manager responsibility for information security

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44386

487 Which of the following should be the FIRST step in developing an information security plan? [44387]

A: Perform a technical vulnerabilities assessment

B: Analyze the current business strategy

C: Perform a business impact analysis

D: Assess the current levels of security awareness

B 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44387

488 When an organization is implementing an information security governance program, its board of

directors should be responsible for: [44388]

A: drafting information security policies.

B: reviewing training and awareness programs.

C: setting the strategic direction of the program.

D: auditing for compliance.

C 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44388

489 Information security projects should be prioritized on the basis of: [44389]

A: time required for implementation.

B: impact on the organization.

C: total cost for implementation.

D: mix of resources required.

B 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44389

490 The MOST important elements to consider when developing a business case for a project is the:

[44390]

A: feasibility and value proposition.

B: resource and time requirements.

C: financial analysis of benefits.

D: alignment with organizational objectives.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44390

491 Achieving compliance with a particular information security standard selected by management

would BEST be described as a: [44391]

A: key goal indicator.

B: critical success factor.

C: key performance indicator.

D: business impact analysis.

C 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44391

492 A risk assessment and business impact analysis (BIA) have been completed for a major proposed

purchase and new process for an organization. There is disagreement between the information

security manager and the business department manager who will own th [44392]

A: Acceptance of the business manager's decision on the risk to the corporation

B: Acceptance of the information security manager's decision on the risk to the corporation

C: Review of the risk assessment with executive management for final input

D: A new risk assessment and BIA are needed to resolve the disagreement

C 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44392

493 An organization has decided to implement bring your own device (BYOD) for laptops and mobile

phones. What should the information security manager focus on FIRST? [44393]

A: Advising against implementing BYOD because of a security risk

B: Preparing a business case for new security tools for BYOD

C: Updating the security awareness program to include BYOD

D: Determining an information security strategy for BYOD

D 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44393

494 An information security manager wants to implement a security information and event

management (SIEM) system not funded in the current budget. Which of the following choices is

MOST likely to persuade management of this need? [44394]

A: A comprehensive risk assessment

B: An enterprise wide impact assessment

C: A well-developed business case

D: Computing the net present value of future savings

C 1

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44394

495 When preparing a business case for the implementation of a security information and event

management (SIEM) system, which of the following should be a PRIMARY driver in the feasibility

study? [44395]

A: Cost of software

B: Cost-benefit analysis

C: Implementation timeframe

D: Industry benchmarks

B 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44395

496 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: [44396]

A: international security standards.

B: risk assessment results.

C: the more stringent requirements.

D: the security organization structure.

C 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44396

497 An organization has consolidated global operations. The chief information officer has asked the

chief information security officer to develop a new organization information security strategy.

Which of the following actions should be taken FIRST? [44397]

A: Identify the assets.

B: Conduct a risk assessment.

C: Define the scope.

D: Perform a business impact analysis.

C 2

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44397

498 To improve the security of an organization's human resources system, an information security

manager was presented with a choice to either implement an additional packet filtering firewall OR

a heuristics-based intrusion detection system. How should the [44398]

A: Risk analysis

B: Business impact analysis

C: Return on investment analysis

D: Cost-benefit analysis

D 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44398

499 A recent audit has identified that security controls required by the organization's policies have not

been implemented for a particular application. What should the information security manager do

NEXT to address this issue? [44399]

A: Discuss the issue with data owners to determine the reason for the exception.

B: Discuss the issue with data custodians to determine the reason for the exception.

C: Report the issue to senior management and request funding to fix the issue.

D: Deny access to the application until the issue is resolved.

A 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44399

500 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? [44400]

A: The information security strategy

B: The information security policy

C: The organization's risk appetite

D: The organization's cost of noncompliance

D 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44400

501 An enterprise has been recently subject to a series of denial-of-service attacks due to a weakness in

security. The information security manager needs to present a business case for increasing the

investment in security. The MOST significant challenge i [44401]

A: explaining technology issues of security.

B: demonstrating value and benefits.

C: simulating various risk scenarios.

D: obtaining benchmarking data for comparison.

B 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44401

502 During a stakeholder meeting, a question was asked regarding who is ultimately accountable for

the protection of sensitive data. Assuming all of the following roles exist in the enterprise, which

would be the MOST appropriate answer? [44402]

A: Security administrators

B: The IT steering committee

C: The board of directors

D: The information security manager

C 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44402

503 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? [44403]

A: Develop a guideline on the acceptable use of social media.

B: Incorporate social media into the security awareness program.

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

D: Employ the use of a web content filtering solution.

A 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44403

504 Implementing a strong password policy is part of an organization's information security strategy

for the year. A business unit believes the strategy may adversely affect a client's adoption of a

recently developed mobile application and has decided not t [44404]

A: Analyze the risk and impact of not implementing the policy.

B: Develop and implement a password policy for the mobile application.

C: Escalate non-implementation of the policy to senior management.

D: Benchmark with similar mobile applications to identify gaps.

A 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44404

505 As an organization grows, exceptions to information security policies that were not originally

specified may become necessary at a later date. In order to ensure effective management of

business risks, exceptions to such policies should be: [44405]

A: considered at the discretion of the information owner.

B: approved by the next higher person in the organizational structure.

C: formally managed within the information security framework.

D: reviewed and approved by the security manager.

C 3

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44405

506 The FIRST action for an information security manager to take when presented with news that new

regulations are being applied to how organizations handle sensitive data is to determine: [44406]

A: processes and activities that may be affected.

B: how senior management would prefer to respond.

C: whether the organization qualifies for an exemption.

D: the approximate cost of compliance.

A 4

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44406

507 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 [44407]

A: Deployment of nested firewalls within the infrastructure

B: Separate security controls for applications, platforms programs and endpoints

C: Multi-factor login requirements for cloud service applications timeouts, and complex passwords

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

B 5

$$1 CIS Information Security 2: 3:

eco\_task\_abbrev Hints

44407

|  |
| --- |
| 119. When creating an incident response plan, the PRIMARY benefit of establishing a clear definition of a security incident is that it helps to: A: communicate the incident response process to stakeholders. B: adequately staff and train incident response teams. C: adequately staff and train incident response teams. D: make tabletop testing more effective.  Answer:B $$ |
| 139. Which of the following is the MOST reliable source of information about emerging information security threats and vulnerabilities? A: A social media group of hackers B: Vulnerability scanning alerts C: Vulnerability scanning alerts D: Threat intelligence groups  Answer:D $$ |
| 141. Which of the following should be an information security manager's PRIMARY role when an organization initiates a data classification process? A: Assign the asset classification level. B: Apply security in accordance with specific classification. C: Define the classification structure to be implemented. D: Verify that assets have been appropriately classified.  Answer:B $$ |
| 99. Which of the following is MOST important to consider when prioritizing threats during the risk assessment process? A: The potential impact on operations B: The capacity of threat actors C: The criticality of threatened systems D: The severity of exploited vulnerabilities  Answer:A $$ |
| 109. Which of the following is the MOST effective approach to communicate general information security responsibilities across an organization? A: Provide regular security awareness training. B: Require staff to sign confidentiality agreements. C: Require staff to sign confidentiality agreements. D: Specify information security responsibilities in job descriptions.  Answer:A $$ |
| 124. Which of the following is the PRIMARY goal of an incident response team during a security incident? A: Minimize disruption to business-critical operations. B: Maintain a documented chain of evidence. C: Maintain a documented chain of evidence. D: Ensure the attackers are detected and stopped.  Answer:A $$ |
| 125. Senior management has decided to accept a significant risk within a security remediation plan. Which of the following is the information security manager's BEST course of action? A: Report the risk acceptance to regulatory agencies. B: Remediate the risk and document the rationale. C: Update the risk register with the risk acceptance. D: Communicate the remediation plan to the board of directors.  Answer:C $$ |
| 146. Which of the following should be an information security manager's PRIMARY focus during the development of a critical system strong highly confidential data? A: Ensuring the amount of residual risk is acceptable B: Reducing the number of vulnerabilities detected C: Reducing the number of vulnerabilities detected D: Complying with regulatory requirements  Answer:C $$ |
| 73. The MOST effective way to communicate the level of impact of information security risks on organizational objectives is to present: A: risk treatment options. B: a risk heat map. C: business impact analysis (BIA) results. D: detailed threat analysis results.  Answer:B $$ |
| 68. Which of the following is MOST likely to increase end user security awareness in organization? A: Security objectives included in job descriptions B: Red team penetration testing C: Simulated phishing attacks D: A dedicated channel for reporting suspicious emails  Answer:C $$ |
| 81. After a security incident has been contained, which of the following should be done FIRST? A: Restore the affected system from backup. B: Conduct forensic analysis. C: Conduct forensic analysis. D: Perform a complete wipe of the affected system.  Answer:A $$ |
| 52. Which of the following should be communicated FIRST to senior management once an information security incident has been contained? A: Details on containment activities B: The initial business impact of the incident  C: Whether the recovery time objective was met D: A summary of key lessons learned from the incident  Answer:B $$ |
| 56. An organization enacted several information security policies to satisfy regulatory requirements. Which of the following situations would MOST likely increase the probability of noncompliance to these requirements? A: Availability of security policy documents a public website B: Lack of training for end users on security policies C: Lack of training for end users on security policies D: Inadequate buy-in from system owners to support the policies  Answer:D $$ |
| 93. Which of the following is the BEST reason to develop comprehensive information security policies? A: To comply with external industry and government regulations B: To gain senior management support for the information security program C: To align the information security program to organizational strategy D: To support development of effective risk indicators  Answer:C $$ |
| 61. When implementing security architecture, an information security manager MUST ensure that security controls: A: are transparent. B: form multiple barriers against threats. C: form multiple barriers against threats. D: are communicated through security policies.  Answer:C $$ |
| 84. A security team is conducting its annual disaster recovery test. Post-restoration testing shows the system response time is significantly slower due to insufficient bandwidth for internet connectivity at the recovery center. Which of the following is the security manager's BEST course of action? A: Document the deficiency for review by business leadership. B: Pursuer risk acceptance for the slower response time. C: Pursuer risk acceptance for the slower response time. D: Reduce the number of applications marked as critical.  Answer:A $$ |
| 55. Which of the following techniques is MOST useful when an incident response team needs to external attacks on multiple corporate network devices? A: Vulnerability assessment of network devices B: Penetration testing of network devices C: Security event correlation analysis D: Endpoint baseline configuration analysis  Answer:C $$ |
| 63. Which of the following is the BEST approach for an information security manager to effectively manage third-party risk? A: Ensure senior management has approved the vendor relationship. B: Ensure risk management efforts are commensurate with risk exposure. C: Ensure vendor governance controls are in place. /  D: Ensure controls are implemented to address changes in risk.  Answer:D $$ |
| 2. What should the information security manager recommend to support the development of a new web application that will allow retail customers to view inventory and order products? A: Implementation of secure transmission protocols B: Request customers adhere to baseline security standards C: Request customers adhere to baseline security standards D: Building an access control matrix  Answer:A $$ |
| . Which of the following provides the BEST evidence that the information security program is aligned to the business strategy? A: The information security team is able to provide key performance indicators (KPIs) to senior management. B: Information security initiatives are directly correlated to business processes. C: Information security initiatives are directly correlated to business processes. D: The information security program manages risk within the business's risk tolerance.  Answer:C $$ |
| . Which of the following MOST effectively helps an organization to align information security governance with corporate governance? A: Developing security performance metrics B: Adopting global security standards to achieve business goals C: Adopting global security standards to achieve business goals D: Prioritizing security initiatives based on IT strategy  Answer:B $$ |
| 17. Which of the following is MOST important for effective communication during incident response? A: Establishing a recovery time objective (RTO) B: Maintaining a  C: Maintaining a relationship with media and law enforcement D: Establishing a mean time to resolve (MTTR) metric  Answer:B $$ |
| 6. An organization recently rolled out a new procurement program that does not include any security requirements. Which of the following should the information security manager do FIRST? A: Conduct security assessments of vendors based on value of annual spend with each vendor. B: Escalate the procurement program gaps to the compliance department in case of noncompliance issues. C: Escalate the procurement program gaps to the compliance department in case of noncompliance issues. D: Ask internal audit to conduct an assessment of the current state of third-party security controls.  Answer:C $$ |
| 40. Which of the following is MOST important for an information security manager to ensure is included in a business case for a new security system? A: Audit-logging capabilities B: Benchmarking results C: Benchmarking results D: Risk reduction associated with the system  Answer:D $$ |
| 45. Which of the following is MOST important to building an effective information security program? A: Logical assess controls for information systems B: Relevant and timely content included in awar ness programs C: Management support for information security D: Information security architecture to increase monitoring activities  Answer:B $$ |
| 39. Which of the following is the BEST reason to separate short-term from long-term plans within an information security roadmap? A: To allocate resources for initiatives B: To allow for reactive initiatives C: To allow for reactive initiatives D: To facilitate business plan reporting to management  Answer:A $$ |
| 49. Which of the following is MOST helpful for prioritizing the recovery of IT assets during a disaster? A: Cost-benefit analysis B: Risk assessment C: Risk assessment D: Business impact analysis (BIA)  Answer:D $$ |
| 34. Recovery time objectives (RTOs) are an output of which of the following? A: Business continuity plan (BCP) B: Disaster recovery plan (DRP) C: Business impact analysis (BIA) D: Service level agreement (SLA)  Answer:B $$ |
| 28. 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: Automation of security controls C: Regular reporting to senior management D: Supportive tone at the top regarding security  Answer:B $$ |
| 30. After adopting an information security framework, an information security manager is working with senior management to change the organization-wide perception that information security is solely the responsibility of the information security department. To achieve this objective, which should be the information security manager's FIRST initiative? A: Develop an information security awareness campaign with senior management's support. B: Document and publish the respobsibilities of the information security department. C: Document and publish the respobsibilities of the information security department. D: Implement a formal process to conduct periodic compliance reviews.  Answer:A $$ |