Isaca.Premium.CISM.VCEup.120q - DEMO

Exam Code: CISM

Exam Name: Certified Information Security Manager

Certification Provider: Isaca

Corresponding Certification: CISM

Website: https://VCEup.com/

Free Exam: https://vceup.com/exam-cism/

Question No: 1

Within a security governance framework, which of the following is the MOST important characteristic of the information security committee? The committee:

A. has a clearly defined charier and meeting protocols.

B. includes a mix of members from all levels of management.

C. conducts frequent reviews of the security policy.

D. has established relationships with external professionals.

Answer: B

Explanation:

Question No: 2

A new program has been implemented to standardize security configurations across a multinational organization Following implementation, the configuration standards should:

A. remain unchanged to avoid variations across the organization

B. be updated to address emerging threats and vulnerabilities.

C. be changed for different subsets of the systems to minimize impact,

D. not deviate from industry best practice baselines.

Answer: B

Explanation:

Question No: 3

Which of the following MOST effectively prevents internal users from modifying sensitive data?

A. Network segmentation

B. Role-based access controls

C. Multi-factor authentication -

D. Acceptable use policies

Answer: B

Explanation:

Question No: 4

Which of the following should be PRIMARILY included in a security training program for business process owners?

A. Application recovery time

B. Impact of security risks

C. Application vulnerabilities

D. List of security incidents reported

Answer: B

Explanation:

Question No: 5

Which of the following is the MOST important consideration when determining the approach for gaining organization-wide acceptance of an information security plan?

A. Mature security policy

B. Information security roles and responsibilities

C. Organizational information security awareness

D. Organizational culture

Answer: D

Explanation:

Question No: 6

To gain a clear understanding of the impact that a new regulatory will have on an organization’s security control, an information manager should FIRST.

A. Conduct a risk assessment

B. Interview senior management

C. Perform a gap analysis

D. Conduct a cost-benefit analysis

Answer: C

Explanation:

Question No: 7

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 information security manager should FIRST.

A. Change the password policy to improve the customer experience

B. Reach alternative secure of identify verification

C. Recommended implementing two-factor authentication.

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

Answer: C

Explanation:

Question No: 8

Which of the following is the BEST method to defend against social engineering attacks?

A. Monitor for unauthorized access attempts and failed logins.

B. Employ the use of a web-content filtering solution.

C. Communicate guideline to limit information posted to public sites

D. Periodically perform antivirus scans to identify malware

Answer: C

Explanation:

Question No: 9

Which of the following is an information security manager's BEST course of action when informed of decision to reduce funding for the information security program?

A. Remove overlapping security controls

B. Prioritize security projects based on risk.

C. Design key risk indicators (KRIs)

D. Create a business case appeal decision.

Answer: B

Explanation:

Question No: 10

What should be information security manager's FIRST course of action when it is discovered a staff member has been posting corporate information on social media sites?

A. Asses the classification of the data posted.

B. Implement controls to block the social media sites.

C. Refer the staff member to the information security policy

D. Notify senior management

Answer: A

Explanation:

Question No: 11

Which of the following would be of GREATEST concern to an information security manager when evaluating a cloud service provider (CSP)?

A. Security controls offered by the provider are inadequate

B. Service level agreements (SLAs) art not well defined.

C. Data retention policies may be violated.

D. There is no right to audit the security of the provider

Answer: B

Explanation:

Question No: 12

Which of the following would BEST justify spending for a compensating control?

A. Risk analysis

B. Vulnerability analysis

C. Threats analysis

D. Peer benchmarking

Answer: C

Explanation:

Question No: 13

A threat intelligence report indicates there has been a significant rise in the number of attacks targeting the industry. What should the information security manager do NEXT?

A. Discuss the risk with senior management.

B. Conduct penetration testing to identity vulnerabilities.

C. Allocate additional resources to monitor perimeter security systems,

D. Update the organization's security awareness campaign.

Answer: A

Explanation:

Question No: 14

During which phase of an incident response process should corrective actions to the response procedure be considered and implemented?

A. Review

B. Identification

C. Eradication

D. Containment

Answer: A

Explanation:

Question No: 15

Which of the following is the BEST way to prevent employees from making unauthorized comments to the media about security incidents in progress?

A. Establish standard media responses for employees to control the message

B. Communicate potential disciplinary actions for noncompliance.

C. Include communication policies In regular information security training

D. training Implement controls to prevent discussion with media during an Incident.

Answer: C

Explanation:

Question No: 16

A company has purchased a rival organization and is looking to integrate security strategies. Which of the following is the GREATEST issue to consider?

A. The organizations have different risk appetites

B. Differing security skills within the organizations

C. Confidential information could be leaked

D. Differing security technologies

Answer: D

Explanation:

Question No: 17

An organization has implemented an enhanced password policy for business applications which requires significantly more business resource to support clients. The BEST approach to obtain the support of business management would be to:

A. Present an analysis of the cost and benefit of the changes

B. Elaborate on the positive impact to information security

C. Present industry benchmarking results to business units

D. Discuss the risk and impact of security incidents if not implemented

Answer: A

Explanation:

Question No: 18

A third-party contract signed by a business unit manager failed to specify information security requirements Which of the following is the BEST way for an information security manager to prevent this situation from reoccurring?

A. Inform business unit management of the information security requirements.

B. Provide information security training to the business units

C. Integrate information security into the procurement process

D. Involve the information security team in contract negotiations

Answer: C

Explanation:

Question No: 19

Which of the following BEST enables an effective escalation process within an incident response program?

A. Dedicated funding for incident management

B. Adequate incident response staffing

C. Monitored program metrics

D. Defined incident thresholds

Answer: D

Explanation:

Question No: 20

Which of the following is the MOST important requirement for the successful implementation of security governance?

A. Mapping to organizational

B. Implementing a security balanced scorecard

C. Performance an enterprise-wide risk assessment

D. Aligning to an international security framework

Answer: A

Explanation:

Question No: 21

Which of the following is the MOST effective way to detect social engineering attacks?

A. Implement real-time monitoring of security-related events.

B. Encourage staff to report any suspicious activities.

C. Implement an acceptable use policy.

D. Provide incident management training to all start.

Answer: B

Explanation:

Question No: 22

Which of the following control type is the FIRST consideration for aligning employee behavior with an organization’s information security objectives?

A. Physical security control

B. Directive security

C. Technical security controls

D. Logical access control

Answer: D

Explanation:

Question No: 23

Which of the following would present the GREATEST need to revise information security poll'

A. Implementation of a new firewall

B. An increase in reported incidents

C. A merger with a competing company

D. Changes in standards and procedures

Answer: C

Explanation:

Question No: 24

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

A. Criticality of the service to the organization

B. Compliance requirements associated with the regulation

C. Compensating controls in place to protect information security

D. Corresponding breaches associated with each vendor

Answer: A

Explanation:

Associated level of risk applied to each vendor is the Residual Risk (the risk after applying vendor's controls). CRISC RM 6th, (Residual Risk = Inherent Risk – Cumulative Effect of Controls) Inherent risk is the current risk without applying any control (i.e. before vendor's controls), this risk is the same quantity in the equation for each vendor. Effect of controls (the value supplied by the vendor) will be different for each vendor. Ex. For vendor 1, Residual Risk1= Inherent/current Risk – Effect of controls of Vendor1 For vendor 2, Residual Risk2= Inherent/current Risk – Effect of controls of Vendor2

Question No: 25

Which of the following is MOST important to the successful development of an information security strategy?

A. An implemented development life cycle process

B. A well-implemented governance framework

C. Current state and desired objectives

D. Approved policies and standards

Answer: C

Explanation:

Question No: 26

When information security management is receiving an increased number of false positive incident reports, which of the following is MOST important to review?

A. The security awareness programs

B. Firewall logs

C. The risk management processes

D. Post-incident analysis results

Answer: D

Explanation:

Question No: 27

Which of the following is the MOST effective approach for integrating security into application development?

A. Including security in user acceptance testing sign-off

B. Performing vulnerability scans

C. Defining security requirements

D. Developing security models in parallel

Answer: C

Explanation:

Question No: 28

Which of the following would contribute MOST to employees' understanding of data handling responsibilities?

A. Demonstrating support by senior management of the security program

B. Implementing a tailored security awareness training program

C. Requiring staff acknowledgement of security policies

D. Labeling documents according to appropriate security classification

Answer: B

Explanation:

Question No: 29

Which of the following is an information security manager's BEST course of action to address a significant materialized risk that was not prevented by organizational controls?

A. Update the business impact analysis (BIA)

B. Update the risk register.

C. Perform root cause analysis.

D. Invoke the incident response plan.

Answer: D

Explanation:

Question No: 30

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

A. Testing information classification controls

B. Determining the controls associated with information classification

C. Maintaining the integrity of data in the information system

D. Deciding what level of classification the information requires

Answer: D

Explanation:

Question No: 31

Which of the following is the BEST resource for evaluating the strengths and weaknesses of an incident response plan?

A. Recovery time objectives (RTOs)

B. Mission, goals and objectives

C. Incident response maturity assessment

D. Documentation from preparedness tests

Answer: D

Explanation:

Question No: 32

Which of the following is the MOST useful metric for determining how well firewall logs are being monitored?

A. The number of port scanning attempts

B. The number of log entries reviewed

C. The number of investigated alerts

D. The number of dropped malformed packets

Answer: C

Explanation:

Question No: 33

Which of the following is the MOST effective data loss control when connecting a personally owned mobile device to the corporate email system?

A. Users must agree to allow the mobile device to be wiped if it is lost

B. Email must be stored in an encrypted format on the mobile device

C. A senior manager must approve each new connection

D. Email synchronization must be prevented when connected to a public Wi-Fi hotspot.

Answer: A

Explanation:

Question No: 34

Which of the following processes is the FIRST step in establishing an information security policy?

A. Review of current global standards

B. Business risk assessment

C. Security controls evaluation

D. Information security audit

Answer: B

Explanation:

Question No: 35

Which of the following would provide the MOST useful input when creating an information security program?

A. Business case

B. Information security budget

C. Key risk indicators (KRIs)

D. Information security strategy

Answer: D

Explanation:

Question No: 36

Which of the following is the PRIMARY reason to invoke continuity and recovery plans?

A. To achieve service delivery objectives

B. To coordinate with senior management

C. To enforce service level agreements (SLAs)

D. To protect corporate networks

Answer: A

Explanation:

Question No: 37

When the inherent risk of a business activity is lower than the acceptable risk level, the BEST course of action would be to:

A. implement controls to mitigate the risk.

B. monitor for business changes.

C. review the residual risk level

D. report compliance to management

Answer: B

Explanation:

Question No: 38

Which of the following would be MOST effective when justifying the cost of adding security controls to an existing web application?

A. Vulnerability assessment results

B. Application security policy

C. A business case

D. Internal audit reports

Answer: C

Explanation:

Question No: 39

Which of the following would BEST assist an information security manager in gaining strategic support from executive management?

A. Risk analysis specific to the organization

B. Research on trends in global information security breaches

C. Rating of the organization s security, based on international standards

D. Annual report of security incidents within the organization

Answer: C

Explanation:

Question No: 40

The PRIMARY reason an organization would require that users sign an acknowledgment of their system access responsibilities is to:

A. assign accountability for transactions made with the user's ID.

B. maintain compliance with industry best practices.

C. serve as evidence of security awareness training.

D. maintain an accurate record of users access rights

Answer: A

Explanation:

Question No: 41

An emergency change was made to an IT system as a result of a failure. Which of the following should be of GREATEST concern to the organizations information security manager?

A. The change did not include a proper assessment of risk.

B. Documentation of the change was made after implementation.

C. The operations team implemented the change without regression testing,

D. The information security manager did not review the change prior to implementation.

Answer: A

Explanation:

Question No: 42

As part of an international expansion plan, an organization has acquired a company located in another jurisdiction. Which of the following would be the BEST way to maintain an effective information security program?

A. Determine new factors that could influence the information security strategy.

B. Implement the current information security program in the acquired company.

C. Merge the two information security programs to establish continuity.

D. Ensure information security s included in any change control efforts

Answer: A

Explanation:

Question No: 43

A policy has been established requiting users to install mobile device management (MDM) software on their personal devices Which of the following would BEST mitigate the risk created by noncompliance with this policy?

A. Disabling remote access from the mobile device

B. Requiring users to sign off on terms and conditions

C. Issuing company-configured mobile devices

D. Issuing warnings and documenting noncompliance

Answer: A

Explanation:

Question No: 44

The PRIMARY purpose of vulnerability assessments is to:

A. provide clear evidence that the system is sufficiently secure.

B. test intrusion detection systems (IDS) and response procedures

C. detect deficiencies that could lead to a system compromise.

D. determine the impact of potential threats,

Answer: C

Explanation:

Question No: 45

Which of the following BEST reduces the likelihood of leakage of private information via email?

A. User awareness training

B. Email encryption

C. Strong user authentication protocols

D. Prohibition on the personal use of email

Answer: B

Explanation:

Question No: 46

The PRIMARY purpose of asset valuation for the management of information security is to:

A. prioritize risk management activities.

B. provide a basis for asset classification.

C. determine the value of each asset

D. eliminate the least significant assets.

Answer: A

Explanation:

Question No: 47

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

A. re-evaluate the risk appetite

B. quantify reputational risks

C. meet information security compliance requirements.

D. ensure appropriate information security governance.

Answer: A

Explanation:

Question No: 48

After implementing an information security governance framework, which of the following would provide the BEST information to develop an information security project plan?

A. Risk heat map

B. Recent audit results

C. Balanced scorecard

D. Gap analysis

Answer: C

Explanation:

Question No: 49

Which of the following is the BEST way to improve the timely reporting of information security incidents?

A. Perform periodic simulations with the incident response team.

B. Regularly reassess and update the incident response plan.

C. Integrate an intrusion detection system (IDS) in the DMZ

D. Incorporate security procedures in help desk processes

Answer: B

Explanation:

Question No: 50

Which of the following processes would BEST help to ensure that information security risks will be evaluated when implementing a new payroll system?

A. Change management

B. Problem management

C. Configuration management

D. Incident management

Answer: A

Explanation:

Question No: 51

When using a newly implemented security information and event management (SIEM) infrastructure, which of the following should be considered FIRST?

A. Encryption

B. Retention

C. Report distribution

D. Tuning

Answer: D

Explanation:

Question No: 52

Which of the following activities BEST enables executive management to ensure value delivery within an information security program?

A. Requiring employees to undergo information security awareness training

B. Assigning an information security manager to a senior management position

C. Approving an industry-recognized information security framework

D. Reviewing business cases for information security initiatives

Answer: D

Explanation:

Question No: 53

The MOST important factors in determining the scope and timing for testing a business continuity plan are:

A. the experience level of personnel and the function location.

B. prior testing results and the degree of detail of the business continuity plan

C. the importance of the function to be tested and the cost of testing,

D. manual processing capabilities and the test location

Answer: C

Explanation:

Question No: 54

An information security manager is concerned that executive management does not support information security initiatives. Which of the following is the BEST way to address this situation?

A. Revise the information security strategy to meet executive management's expectations.

B. Escalate noncompliance concerns to the internal audit manager

C. Report the risk and status of the information security program to the board.

D. Demonstrate alignment of the information security function with business needs.

Answer: D

Explanation:

Question No: 55

An information security manager is concerned that executive management does not su the following is the BEST way to address this situation?

A. Revise the information security strategy to meet executive management expectations.

B. Escalate noncompliance concerns to the internal audit manager

C. Report the risk and status of the information security program to the board.

D. Demonstrate alignment of the information security function with business needs.

Answer: D

Explanation:

Question No: 56

The PRIMARY benefit of integrating information security activities into change management processes is to:

A. provide greater accountability for security-related changes In the business

B. protect the organization from unauthorized changes.

C. protect the business from collusion and compliance threats.

D. ensure required controls are Included in changes.

Answer: B

Explanation:

Question No: 57

Which of the following provides the BEST input to maintain an effective asset classification program?

A. Business impact analysis (BIA)

B. Annual toss expectancy

C. Vulnerability assessment

D. Risk heat map

Answer: A

Explanation:

Question No: 58

A contract bid is digitally signed and electronically mailed The PRIMARY advantage to using a digital signature is that

A. any alteration of the bid will invalidate the signature.

B. the signature can be authenticated even if no encryption is used,

C. the bid cannot be forged even if the keys are compromised.

D. the bid and the signature can be copied from one document to another

Answer: B

Explanation:

Question No: 59

An organization's security policy is to disable access to USB storage devices on laptops and desktops.

Which of the following is the STRONGEST justification foi granting an exception to the policy?

A. Access is restricted to read-only.

B. USB storage devices are enabled based on user roles

C. Users accept the risk of noncompliance.

D. The benefit is greater than the potential risk

Answer: D

Explanation:

Question No: 60

The GREATEST benefit of choosing a private cloud over a public cloud would be:

A. containment of customer data

B. collection of data forensic

C. online service availability.

D. server protection.

Answer: A

Explanation:

Question No: 61

An access rights review revealed that some former employees' access is still active. Once the access is revoked, which of the following is the BEST course of action to help prevent recurrence?

A. Implement a periodic recertification program.

B. Initiate an access control policy review.

C. Validate HR offboarding processes.

D. Conduct a root cause analysis.

Answer: A

Explanation:

Question No: 62

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

A. Recognised threat intelligence communities

B. Open-source reconnaissance

C. Disaster recovery consultants widely endorsed in industry forums

D. Incident response experts from highly regarded peer organizations

Answer: A

Explanation:

Question No: 63

Which of the following will BEST protect an organization against spear phishing?

A. Antivirus software

B. Acceptable use policy

C. Email content filtering

D. End-user training

Answer: D

Explanation:

Question No: 64

Which of the following is the PRIMARY reason social media has become a popular target for attack?

A. The reduced effectiveness of access controls

B. The accessibility of social media from multiple locations

C. The prevalence of strong perimeter protection

D. The element of trust created by social media

Answer: D

Explanation:

Question No: 65

Which of the following is the BEST way to demonstrate to senior management that organizational security practices comply with industry standards?

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

Answer: D

Explanation:

Question No: 66

To ensure appropriate control of information processed in IT systems, security safeguards should be based PRIMARILY on:

A. criteria consistent with classification levels

B. efficient technical processing considerations,

C. overall IT capacity and operational constraints,

D. established guidelines

Answer: A

Explanation:

Question No: 67

Which of the following is the PRIMARY objective of a business impact analysis (BIA):

A. Define the recovery point objective (RPO).

B. Determine recovery priorities.

C. Confirm control effectiveness.

D. Analyze vulnerabilities

Answer: A

Explanation:

Topic 2, Exam Pool B

Question No: 68

Which of the following BEST indicates senior management support for an information security program?

A. Detailed information security policies are established and regularly reviewed.

B. The information security manager meets regularly with the lines of business.

C. Key performance indicators (KPIs) are defined for the information security program.

D. Risk assessments are conducted frequently by the information security team.

Answer: A

Explanation:

Question No: 69

An information security manager suspects that the organization has suffered a ransomware attack.

What should be done FIRST

A. Notify senior management

B. Alert employees to the attack.

C. Confirm the infection.

D. Isolate the affected systems.

Answer: D

Explanation:

Question No: 70

An information security manager is reviewing the impact of a regulation on the organization’s human resources system. The NEXT course of action should be to:

A. perform a gap analysis of compliance requirements

B. assess the penalties for noncompliance.

C. review the organization s most recent audit report

C. determine the cost of compliance

Answer: A

Explanation:

Question No: 71

A new regulation has been announced that requires mandatory reporting of security incidents that affect personal client information. Which of the following should be the information security manager's FIRST course of action?

A. Inform senior management of the new regulation.

B. Review the current security policy.

C. Update the security incident management process

D. Determine impact to me business

Answer: D

Explanation:

Question No: 72

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 to implement the policy. Which of the following is the information security manager s BEST course of action?

A. Analyze the risk and impact of not implementing the policy.

B. Develop and implement a password policy for d mobile application

C. Escalate non-implementation of the policy to senior management

D. Benchmark with similar mobile applications to identify gaps

Answer: A

Explanation:

Question No: 73

Which of the following contributes MOST to the effective implementation of an information security strategy?

A. Reporting of security metrics

B. Regular security awareness training

C. Endorsement by senior management

D. Implementation of security standards

Answer: C

Explanation:

Question No: 74

An information security manager determines the organizations critical systems may be vulnerable to a new zero-day attack. The FIRST course of action is to:

A. analyze the probability of compromise

B. re-assess the firewall configuration

C. advise management of risk and remediation cost

D. survey peer organizations to see how they have addressed the issue.

Answer: A

Explanation:

Question No: 75

The MAIN reason for internal certification of web-based business applications is to ensure:

A. compliance with industry standards-

B. changes to the organizational policy framework are identified,

C. up-to-date web technology is being used.

D. compliance with organizational policies.

Answer: D

Explanation:

Question No: 76

Knowing which of the following is MOST important when the information security manager is seeking senior management commitment?

A. Security costs

B. Technical vulnerabilities

C. Security technology requirements

D. Implementation tasks

Answer: D

Explanation:

Question No: 77

Which of the following is MOST critical for prioritizing actions in a business continuity plan (BCP)?

A. Risk assessment

B. Business impact analysis (BIA)

C. Asset classification

D. Business process mapping

Answer: B

Explanation:

Question No: 78

Which of the following is the BEST way for an information security manager to identify compliance with information security policies within an organization?

A. Conduct security awareness testing

B. Perform vulnerability assessments

C. Analyze system logs

D. Conduct per iodic audits.

Answer: D

Explanation:

Question No: 79

Which of the following is the MOST effective defense against spear phishing attacks?

A. Unified threat management

B. Web filtering

C. Anti-spam solution

D. User awareness training

Answer: D

Explanation:

Question No: 80

Which of the following is MOST important to enable after completing action plan?

A. Threat profile

B. Inherent risk

C. Residual risk

D. Vulnerability landscape

Answer: C

Explanation:

Question No: 81

Which of the following would BEST enable an organization to effectively monitor the implementation of standardized configurations?

A. Implement a separate change tracking system to record changes to configurations.

B. Perform periodic audits to detect non-com pliant configurations.

C. Develop policies requiring use of the established benchmarks.

D. Implement automated scanning against the established benchmarks.

Answer: D

Explanation:

Question No: 82

What is the MAIN reason for an organization to develop an incident response plan?

Identify training requirements for the incident response team.

Priorities treatment based on incident critically.

What is the MAIN reason for an organization to develop an incident response plan?

A. Identity training requirements for the incident response team.

B. Prioritize treatment based on incident criticality.

C. Trigger immediate recovery procedures.

D. Provide a process for notifying stakeholders of trie incident.

Answer: C

Explanation:

Question No: 83

The PRIMARY benefit of integrating information security risk into enterprise risk management is to:

A. ensure timely risk mitigation.

B. justify the information security budget

C. obtain senior management’s commitment.

D. provide a holistic view of risk

Answer: D

Explanation:

Question No: 84

Which of the following should be the information security manager's NEXT step following senior management approval of the information security strategy?

A. Develop a security pokey.

B. Develop a budget

C. Perform a gap analysis.

D. Form a steering committee

Answer: D

Explanation:

Question No: 85

Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?

A. Implement more stringent countermeasures.

B. Evaluate whether an excessive level of control is being applied.

C. Ask senior management to increase the acceptable risk levels

D. Ask senior management to lower the acceptable risk levels.

Answer: B

Explanation:

Question No: 86

Before final acceptance of residual risk, what is the BEST way for an information security manager to address risk factors determined to be lower than acceptable risk levels?

A. Implement more stringent countermeasures.

B. Evaluate whether an excessive level of control is being applied.

C. Ask senior management to increase the acceptable risk levels

D. Ask senior management to lower the acceptable risk levels

Answer: B

Explanation:

Question No: 87

A newly hired information security manager discovers that the cleanup of accounts for terminated employees happens only once a year. Which of the following should be the information security manager's FIRST course of action?

A. Design and document a new process

B. Update the security policy

C. Perform a risk assessment

D. Report the issue to senior management

Answer: D

Explanation:

Question No: 88

An organization has recently experienced unauthorized device access to its network. To proactively manage the problem and mitigate this risk, the BEST preventive control would be to:

A. keep an inventory of network and hardware addresses of all systems connected to the network

B. implement network-level authentication and login to regulate access of devices to the network

C. deploy an automated asset inventory discovery tool to identify devices that access the network

D. install a stateful inspection firewall to prevent unauthorized network traffic

Answer: C

Explanation:

Question No: 89

What is the MOST important consideration when establishing metrics for reporting to the information security strategy committee?

A. Agreeing on baseline values for the metrics

B. Developing a dashboard for communicating the metrics

C. Providing real-time insight on the security posture of the organization

D. Benchmarking the expected value of the metrics against industry standards

Answer: C

Explanation:

Question No: 90

When developing a disaster recovery plan, which of the following would be MOST helpful in prioritizing the order in which systems should be recovered?

A. Reviewing the business strategy

B. Reviewing the information security policy

C. Performing a business impact analysis (BIA)

D. Measuring the volume of data in each system

Answer: C

Explanation:

Question No: 91

Which of the following is the BEST approach for encouraging business units to assume their roles and responsibilities in an information security program?

A. Perform a risk assessment

B. Conduct an awareness program

C. Conduct a security audit.

D. Develop controls and countermeasures

Answer: C

Explanation:

Question No: 92

Which of the following activities should take place FIRST when a security patch for Internet software is received from a vendor?

A. The patch should be applied to critical systems.

B. The patch should be validated using a hash algorithm.

C. The patch should be evaluated in a testing environment.

D. The patch should be deployed quickly to systems that are vulnerable.

Answer: C

Explanation:

Question No: 93

For a business operating in a competitive and evolving online market, it is MOST important for a security policy to focus on:

A. defining policies for new technologies.

B. enabling adoption of new Technologies.

C. requiring accreditation for new technologies.

D. managing risks of new technologies

Answer: B

Explanation:

Question No: 94

When developing an incident response plan, which of the following is the MOST -effective way to ensure incidents common to the organization are handled properly?

A. Adopting industry standard response procedures

B. Rehearsing response scenarios

C. Conducting awareness training

D. Creating and distributing a personnel call tree

Answer: A

Explanation:

Question No: 95

Following a successful and well-publicized hacking incident, an organization alias plans to improve application security. Which of the following is a security project risk?

A. Critical evidence may be lost.

B. The reputation of the organization may be damaged

C. A trapdoor may have been installed m the application.

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

Answer: D

Explanation:

Question No: 96

What should be an organization'«. MAIN concern when evaluating an Infrastructure as a Service

(laaS) cloud computing model for an e-commerce application?

A. Internal audit requirements

B. Availability of providers services

C. Where the application resides

D. Application ownership

Answer: B

Explanation:

Question No: 97

Which of the following would be MOST effective in ensuring that information security is appropriately addressed in new systems?

A. Information security staff perform compliance reviews before production begins

B. Information security staff take responsibility for the design of system security

C. Internal audit signs off on security prior to implementation

D. Business requirements must include security objectives.

Answer: D

Explanation:

Question No: 98

A multinational organization wants to ensure its privacy program appropriately addresses privacy risk throughout its operations. Which of the following would be of MOST concern to senior management?

A. The organization uses a decentralized privacy governance structure

B. Privacy policies ire only reviewed annually

C. The organization doe* not have a dedicated privacy officer

D. The privacy program does not include a formal warning component

Answer: A

Explanation:

Question No: 99

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

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

Answer: A

Explanation:

Question No: 100

After an information security business case has been approved by senior management, it should be:

A. used to design functional requirements for the solution

B. used as the foundation for a risk assessment

C. referenced to build architectural blueprints for the solution

D. reviewed at key intervals to ensure intended outcomes.

Answer: A

Explanation:

Question No: 101

Which is MOST important to enable a timely response to a security breach?

A. Knowledge sharing and collaboration

B. Security event logging

C. Roles and responsibilities

D. Forensic analysis

Answer: C

Explanation:

Question No: 102

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?

A. Cost of software

B. Cost-benefit analysis

C. Implementation timeframe

D. Industry benchmarks

Answer: B

Explanation:

Question No: 103

Which of the following BEST demonstrates that an organization supports information security governance?

A. Employees attend annual organization-wide security training.

B. Information security policies are readily available to employees.

C. The incident response plan is documented and tested regularly.

D. Information security steering committee meetings are held regularly.

Answer: D

Explanation:

Question No: 104

Executive management is considering outsourcing all IT operations. Which of the following functions should remain internal?

A. Data encryption

B. Data ownership

C. Data custodian

D. Data monitoring

Answer: B

Explanation:

Question No: 105

Which of the following is the MOST important outcome from vulnerability scanning?

A. Prioritization of risks

B. Information about steps necessary to hack the system

C. Identification of back doors

D. Verification that systems are property configured

Answer: C

Explanation:

Question No: 106

The MOST likely cause of a security information event monitoring (SIEM) solution failing to identify a serious incident is that the system:

A. has not been updated with the latest patches

B. is hosted by a cloud service provider

C. has performance issues

D. is not collecting logs from relevant devices.

Answer: D

Explanation:

Question No: 107

Which of the following should be the PRIMARY expectation of management when an organization introduces an information security governance framework?

A. Optimized information security resources

B. Consistent execution of information security strategy

C. Improved accountability to shareholders

D. Increased influence of security management

Answer: C

Explanation:

Question No: 108

Which of the following is MOST critical to review when preparing to outsource a data repository to a cloud-based solution?

A. Disaster recovery plan

B. Identity and access management

C. Vendor's information security policy

D. A risk assessment

Answer: D

Explanation:

Question No: 109

When developing a new application, which of the following is the BEST approach to ensure compliance with security requirements?

A. Provide security training for developers.

B. Prepare detailed acceptance criteria

C. Adhere to change management processes.

D. Perform a security gap analysis.

Answer: A

Explanation:

Question No: 110

Which of the following is the BKT approach for an information security manager when developing new information security policies?

A. Create a stakeholder nap

B. Reference an industry standard.

C. Establish an information security governance committee

D. Download a policy template

Answer: C

Explanation:

Question No: 111

Which of the following is the MOST important step in risk ranking?

A. Threat assessment

B. Mitigation cost

C. Vulnerability analysis

D. Impact assessment

Answer: D

Explanation:

Question No: 112

Due lo budget constraints, an internal IT application does not include the necessary controls to meet a client service level agreement (SLA). Which of the following is the information security manager's BEST course of action?

A. Inform the legal department of the deficiency

B. Analyze and report the issue to server management

C. Require the application owner to implement the controls.

D. Assess and present the risks to the application owner

Answer: B

Explanation:

Question No: 113

Business units within an organization are resistant to proposed changes to the information security program. Which of the following is the BEST way to address this issue?

A. Communicating critical risk assessment results to business unit managers

B. Including business unit representation on the security steering committee

C. Publishing updated information security policies

D. Implementing additional security awareness training

Answer: B

Explanation:

Question No: 114

Which of the following is the BEST reason to reassess risk following an incident?

A. To capture lessons learned

B. To update changes in the threat environment

C. To update roles and responsibilities

D. To accurately document risk to the organization

Answer: B

Explanation:

Question No: 115

A third-party service provider has proposed a data loss prevention (DLP) solution. Which of the following MUST be in place for this solution to be relevant to the organization?

A. Senior management support

B. An adequate data testing environment

C. A business case

D. A data classification schema

Answer: C

Explanation:

Question No: 116

An organization is MOST at risk from a new worm being introduced through the intranet when:

A. desktop virus definition files are not up to date

B. system software does not undergo integrity checks.

C. hosts have static IP addresses.

D. executable code is run from inside the firewall

Answer: B

Explanation:

Question No: 117

Which of the following is the MOST important reason for performing vulnerability assessments periodically?

A. The current threat levels are being assessed.

B. Technology risks must be mitigated.

C. The environment changes constantly.

D. Management requires regular reports.

Answer: C

Explanation:

Question No: 118

Which of the following is the MOST effective way to identify changes in an information security environment?

A. Continuous monitoring

B. Security baselining

C. Annual risk assessments

D. Business impact analysts

Answer: A

Explanation:

Question No: 119

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

A. Analyze penetration test results.

B. Analyze recent security risk assessments.

C. Analyze vulnerability assessments.

D. Analyze security anomalies.

Answer: A

Explanation:

Question No: 120

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

A. Review vulnerability assessment

B. Conduct a security audit

C. Initiate modem response

D. Isolate the system.

Answer: C

Explanation: