

ECCouncil.712-50.by,Isac,173q

Number: 712-50
Passing Score: 800
Time Limit: 120
File Version: 11.0

Exam Code: 712-50
Exam Name: EC-Council Certified CISO



Exam A

QUESTION 1

A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

- A. The auditors have not followed proper auditing processes
- B. The CIO of the organization disagrees with the finding
- C. The risk tolerance of the organization permits this risk
- D. The organization has purchased cyber insurance

Correct Answer: C

Section:

QUESTION 2

The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

- A. The asset is more expensive than the remediation
- B. The audit finding is incorrect
- C. The asset being protected is less valuable than the remediation costs
- D. The remediation costs are irrelevant; it must be implemented regardless of cost.



Correct Answer: C

Section:

QUESTION 3

When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

- A. Transfer financial resources from other critical programs
- B. Take the system off line until the budget is available
- C. Deploy countermeasures and compensating controls until the budget is available
- D. Schedule an emergency meeting and request the funding to fix the issue

Correct Answer: C

Section:

QUESTION 4

An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.

- A. Install software patch, Operate system, Maintain system
- B. Discover software, Remove affected software, Apply software patch
- C. Install software patch, configuration adjustment, Software Removal
- D. Software removal, install software patch, maintain system

Correct Answer: C

Section:

QUESTION 5

When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

- A. Threat Level, Risk of Compromise, and Consequences of Compromise
- B. Risk Avoidance, Threat Level, and Consequences of Compromise
- C. Risk Transfer, Reputational Impact, and Consequences of Compromise
- D. Reputational Impact, Financial Impact, and Risk of Compromise

Correct Answer: A

Section:

QUESTION 6

The effectiveness of an audit is measured by?

- A. The number of actionable items in the recommendations
- B. How it exposes the risk tolerance of the company
- C. How the recommendations directly support the goals of the company
- D. The number of security controls the company has in use

Correct Answer: C

Section:

QUESTION 7

A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

- A. Have internal audit conduct another audit to see what has changed.
- B. Contract with an external audit company to conduct an unbiased audit
- C. Review the recommendations and follow up to see if audit implemented the changes
- D. Meet with audit team to determine a timeline for corrections

Correct Answer: C

Section:

QUESTION 8

A missing/ineffective security control is identified. Which of the following should be the NEXT step?

- A. Perform an audit to measure the control formally
- B. Escalate the issue to the IT organization
- C. Perform a risk assessment to measure risk
- D. Establish Key Risk Indicators

Correct Answer: C

Section:



QUESTION 9

The risk found after a control has been fully implemented is called:

- A. Residual Risk
- B. Total Risk
- C. Post implementation risk
- D. Transferred risk

Correct Answer: A

Section:

QUESTION 10

In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

- A. Internal Audit
- B. Database Administration
- C. Information Security
- D. Compliance

Correct Answer: C

Section:

QUESTION 11

At which point should the identity access management team be notified of the termination of an employee?

- A. At the end of the day once the employee is off site
- B. During the monthly review cycle
- C. Immediately so the employee account(s) can be disabled
- D. Before an audit

Correct Answer: C

Section:

QUESTION 12

Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

- A. Strong authentication technologies
- B. Financial reporting regulations
- C. Credit card compliance and regulations
- D. Local privacy laws

Correct Answer: D

Section:

QUESTION 13

You have implemented a new security control. Which of the following risk strategy options have you engaged in?

- A. Risk Avoidance
- B. Risk Acceptance
- C. Risk Transfer
- D. Risk Mitigation

Correct Answer: D
Section:

QUESTION 14

You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

- A. Risk Avoidance
- B. Risk Acceptance
- C. Risk Transfer
- D. Risk Mitigation

Correct Answer: C
Section:

QUESTION 15

Risk that remains after risk mitigation is known as

- A. Persistent risk
- B. Residual risk
- C. Accepted risk
- D. Non-tolerated risk

Correct Answer: B
Section:

QUESTION 16

After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

- A. Risk Tolerance
- B. Qualitative risk analysis
- C. Risk Appetite
- D. Quantitative risk analysis

Correct Answer: D
Section:

QUESTION 17

When dealing with a risk management process, asset classification is important because it will impact the overall:

- A. Threat identification
- B. Risk monitoring
- C. Risk treatment



D. Risk tolerance

Correct Answer: C

Section:

QUESTION 18

Which of the following intellectual Property components is focused on maintaining brand recognition?

- A. Trademark
- B. Patent
- C. Research Logs
- D. Copyright

Correct Answer: A

Section:

QUESTION 19

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

- A. Due Protection
- B. Due Care
- C. Due Compromise
- D. Due process

Correct Answer: B

Section:

QUESTION 20

When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

- A. How many credit card records are stored?
- B. How many servers do you have?
- C. What is the scope of the certification?
- D. What is the value of the assets at risk?

Correct Answer: C

Section:

QUESTION 21

What is a difference from the list below between quantitative and qualitative Risk Assessment?

- A. Quantitative risk assessments result in an exact number (in monetary terms)
- B. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
- C. Qualitative risk assessments map to business objectives
- D. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Correct Answer: A



Section:

QUESTION 22

What is the definition of Risk in Information Security?

- A. Risk = Probability x Impact
- B. Risk = Threat x Probability
- C. Risk = Financial Impact x Probability
- D. Risk = Impact x Threat

Correct Answer: A

Section:

QUESTION 23

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

- A. They are objective and can express risk / cost in real numbers
- B. They are subjective and can be completed more quickly
- C. They are objective and express risk / cost in approximates
- D. They are subjective and can express risk /cost in real numbers

Correct Answer: A

Section:

QUESTION 24

Which of the following is MOST important when dealing with an Information Security Steering committee:

- A. Include a mix of members from different departments and staff levels.
- B. Ensure that security policies and procedures have been vetted and approved.
- C. Review all past audit and compliance reports.
- D. Be briefed about new trends and products at each meeting by a vendor.

Correct Answer: C

Section:

QUESTION 25

A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

- A. Enforce the existing security standards and do not allow the deployment of the new technology.
- B. Amend the standard to permit the deployment.
- C. If the risks associated with that technology are not already identified, perform a risk analysis to quantify the risk, and allow the business unit to proceed based on the identified risk level.
- D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

Correct Answer: C

Section:



QUESTION 26

The PRIMARY objective of security awareness is to:

- A. Ensure that security policies are read.
- B. Encourage security-conscious employee behavior.
- C. Meet legal and regulatory requirements.
- D. Put employees on notice in case follow-up action for noncompliance is necessary

Correct Answer: B

Section:

QUESTION 27

Which of the following is MOST likely to be discretionary?

- A. Policies
- B. Procedures
- C. Guidelines
- D. Standards

Correct Answer: C

Section:

QUESTION 28

Why is it vitally important that senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

Correct Answer: A

Section:

QUESTION 29

When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

- A. When there is a need to develop a more unified incident response capability.
- B. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.
- C. When there is a variety of technologies deployed in the infrastructure.
- D. When it results in an overall lower cost of operating the security program.

Correct Answer: B

Section:

QUESTION 30

What is the relationship between information protection and regulatory compliance?



- A. That all information in an organization must be protected equally.
- B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
- C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.
- D. There is no relationship between the two.

Correct Answer: C

Section:

QUESTION 31

Regulatory requirements typically force organizations to implement

- A. Mandatory controls
- B. Discretionary controls
- C. Optional controls
- D. Financial controls

Correct Answer: A

Section:

QUESTION 32

When managing the security architecture for your company you must consider:

- A. Security and IT Staff size
- B. Company Values
- C. Budget
- D. All of the above

Correct Answer: D

Section:

QUESTION 33

If your organization operates under a model of "assumption of breach", you should:

- A. Protect all information resource assets equally
- B. Establish active firewall monitoring protocols
- C. Purchase insurance for your compliance liability
- D. Focus your security efforts on high value assets

Correct Answer: C

Section:

QUESTION 34

A method to transfer risk is to:

- A. Implement redundancy
- B. move operations to another region
- C. purchase breach insurance



D. Alignment with business operations

Correct Answer: C

Section:

QUESTION 35

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

- A. Controlled mitigation effort
- B. Risk impact comparison
- C. Relative likelihood of event
- D. Comparative threat analysis

Correct Answer: C

Section:

QUESTION 36

Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

- A. Risk management
- B. Security management
- C. Mitigation management
- D. Compliance management

Correct Answer: D

Section:

QUESTION 37

A security manager regularly checks work areas after business hours for security violations; such as unsecured files or unattended computers with active sessions. This activity BEST demonstrates what part of a security program?

- A. Audit validation
- B. Physical control testing
- C. Compliance management
- D. Security awareness training

Correct Answer: C

Section:

QUESTION 38

A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected. Who must be informed of this incident?

- A. Internal audit
- B. The data owner
- C. All executive staff
- D. Government regulators



Correct Answer: B

Section:

QUESTION 39

A company wants to fill a Chief Information Security Officer position in the organization. They need to define and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

- A. Multiple certifications, strong technical capabilities and lengthy resume
- B. Industry certifications, technical knowledge and program management skills
- C. College degree, audit capabilities and complex project management
- D. Multiple references, strong background check and industry certifications

Correct Answer: B

Section:

QUESTION 40

An organization licenses and uses personal information for business operations, and a server containing that information has been compromised. What kind of law would require notifying the owner or licensee of this incident?

- A. Data breach disclosure
- B. Consumer right disclosure
- C. Security incident disclosure
- D. Special circumstance disclosure

Correct Answer: A

Section:

QUESTION 41

An organization's firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

- A. A high threat environment
- B. A low risk tolerance environment
- C. A low vulnerability environment
- D. A high risk tolerance environment

Correct Answer: D

Section:

QUESTION 42

An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?

- A. Determine the risk tolerance
- B. Perform an asset classification
- C. Create an architecture gap analysis
- D. Analyze existing controls on systems



Correct Answer: B

Section:

QUESTION 43

A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

- A. Providing a risk program governance structure
- B. Ensuring developers include risk control comments in code
- C. Creating risk assessment templates based on specific threats
- D. Allowing for the acceptance of risk for regulatory compliance requirements

Correct Answer: A

Section:

QUESTION 44

Which of the following international standards can be BEST used to define a Risk Management process in an organization?

- A. National Institute for Standards and Technology 800-50 (NIST 800-50)
- B. International Organization for Standardizations – 27005 (ISO-27005)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations – 27004 (ISO-27004)

Correct Answer: B

Section:

QUESTION 45

An organization is looking for a framework to measure the efficiency and effectiveness of their Information Security Management System. Which of the following international standards can BEST assist this organization?

- A. International Organization for Standardizations – 27004 (ISO-27004)
- B. Payment Card Industry Data Security Standards (PCI-DSS)
- C. Control Objectives for Information Technology (COBIT)
- D. International Organization for Standardizations – 27005 (ISO-27005)

Correct Answer: A

Section:

QUESTION 46

A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

- A. Information Technology Infrastructure Library (ITIL)
- B. International Organization for Standardization (ISO) standards
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. National Institute for Standards and Technology (NIST) standard

Correct Answer: C

Section:



QUESTION 47

A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

- A. International Organization for Standardizations – 22301 (ISO-22301)
- B. Information Technology Infrastructure Library (ITIL)
- C. Payment Card Industry Data Security Standards (PCI-DSS)
- D. International Organization for Standardizations – 27005 (ISO-27005)

Correct Answer: A

Section:

QUESTION 48

A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

- A. Compliance to the Payment Card Industry (PCI) regulations.
- B. Alignment with financial reporting regulations for each country where they operate.
- C. Alignment with International Organization for Standardization (ISO) standards.
- D. Compliance with patient data protection regulations for each country where they operate.

Correct Answer: D

Section:

QUESTION 49

The patching and monitoring of systems on a consistent schedule is required by?

- A. Local privacy laws
- B. Industry best practices
- C. Risk Management frameworks
- D. Audit best practices

Correct Answer: C

Section:

QUESTION 50

As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

- A. Executive summary
- B. Penetration test agreement
- C. Names and phone numbers of those who conducted the audit
- D. Business charter

Correct Answer: A

Section:

QUESTION 51

As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to



take breaks outside. Upon looking closer you see there is no badge reader.
What should you do?

- A. Nothing, this falls outside your area of influence.
- B. Close and chain the door shut and send a company-wide memo banning the practice.
- C. Have a risk assessment performed.
- D. Post a guard at the door to maintain physical security

Correct Answer: C
Section:

QUESTION 52

Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

- A. Detective Controls
- B. Proactive Controls
- C. Preemptive Controls
- D. Organizational Controls

Correct Answer: D
Section:

QUESTION 53

The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team.
This is consider a bad practice MAINLY because

- A. The IT team is not familiar in IT audit practices
- B. This represents a bad implementation of the Least Privilege principle
- C. This represents a conflict of interest
- D. The IT team is not certified to perform audits

Correct Answer: C
Section:

QUESTION 54

The BEST organization to provide a comprehensive, independent and certifiable perspective on established security controls in an environment is

- A. Penetration testers
- B. External Audit
- C. Internal Audit
- D. Forensic experts

Correct Answer: B
Section:

QUESTION 55

While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

- A. Enterprise Risk Assessment
- B. Disaster recovery strategic plan
- C. Business continuity plan
- D. Application mapping document

Correct Answer: B

Section:

QUESTION 56

Security related breaches are assessed and contained through which of the following?

- A. The IT support team.
- B. A forensic analysis.
- C. Incident response
- D. Physical security team.

Correct Answer: C

Section:

QUESTION 57

Which of the following backup sites takes the longest recovery time?

- A. Cold site
- B. Hot site
- C. Warm site
- D. Mobile backup site

Correct Answer: A

Section:

QUESTION 58

What is the FIRST step in developing the vulnerability management program?

- A. Baseline the Environment
- B. Maintain and Monitor
- C. Organization Vulnerability
- D. Define Policy

Correct Answer: A

Section:

QUESTION 59

An organization has implemented a change management process for all changes to the IT production environment. This change management process follows best practices and is expected to help stabilize the availability and integrity of the organization's IT environment. Which of the following can be used to measure the effectiveness of this newly implemented process:

- A. Number of change orders rejected



- B. Number and length of planned outages
- C. Number of unplanned outages
- D. Number of change orders processed

Correct Answer: C

Section:

QUESTION 60

Which of the following is the MOST effective way to measure the effectiveness of security controls on a perimeter network?

- A. Perform a vulnerability scan of the network
- B. External penetration testing by a qualified third party
- C. Internal Firewall ruleset reviews
- D. Implement network intrusion prevention systems

Correct Answer: B

Section:

QUESTION 61

Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

- A. Security Administrators
- B. Internal/External Audit
- C. Risk Management
- D. Security Operations

Correct Answer: B

Section:

QUESTION 62

To have accurate and effective information security policies how often should the CISO review the organization policies?

- A. Every 6 months
- B. Quarterly
- C. Before an audit
- D. At least once a year

Correct Answer: D

Section:

QUESTION 63

How often should an environment be monitored for cyber threats, risks, and exposures?

- A. Weekly
- B. Monthly
- C. Quarterly
- D. Daily



Correct Answer: D

Section:

QUESTION 64

Which is the BEST solution to monitor, measure, and report changes to critical data in a system?

- A. Application logs
- B. File integrity monitoring
- C. SNMP traps
- D. Syslog

Correct Answer: B

Section:

QUESTION 65

When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

- A. Daily
- B. Hourly
- C. Weekly
- D. Monthly

Correct Answer: A

Section:

QUESTION 66

Which represents PROPER separation of duties in the corporate environment?

- A. Information Security and Identity Access Management teams perform two distinct functions
- B. Developers and Network teams both have admin rights on servers
- C. Finance has access to Human Resources data
- D. Information Security and Network teams perform two distinct functions

Correct Answer: D

Section:

QUESTION 67

Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?

- A. Servers, routers, switches, modem
- B. Firewall, exchange, web server, intrusion detection system (IDS)
- C. Firewall, anti-virus console, IDS, syslog
- D. IDS, syslog, router, switches

Correct Answer: C

Section:



QUESTION 68

Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

- A. All vulnerabilities found on servers and desktops
- B. Only critical and high vulnerabilities on servers and desktops
- C. Only critical and high vulnerabilities that impact important production servers
- D. All vulnerabilities that impact important production servers

Correct Answer: C

Section:

QUESTION 69

You have implemented the new controls. What is the next step?

- A. Document the process for the stakeholders
- B. Monitor the effectiveness of the controls
- C. Update the audit findings report
- D. Perform a risk assessment

Correct Answer: B

Section:

QUESTION 70

An audit was conducted and many critical applications were found to have no disaster recovery plans in place. You conduct a Business Impact Analysis (BIA) to determine impact to the company for each application. What should be the NEXT step?

- A. Determine the annual loss expectancy (ALE)
- B. Create a crisis management plan
- C. Create technology recovery plans
- D. Build a secondary hot site

Correct Answer: C

Section:

QUESTION 71

Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

- A. Control Objective for Information Technology (COBIT)
- B. Committee of Sponsoring Organizations (COSO)
- C. Payment Card Industry (PCI)
- D. Information Technology Infrastructure Library (ITIL)

Correct Answer: A

Section:

QUESTION 72

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

- A. Plan-Check-Do-Act
- B. Plan-Do-Check-Act
- C. Plan-Select-Implement-Evaluate
- D. SCORE (Security Consensus Operational Readiness Evaluation)

Correct Answer: B

Section:

QUESTION 73

Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

- A. To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in their organization.
- B. To provide a common basis for developing organizational security standards
- C. To provide effective security management practice and to provide confidence in interorganizational dealings
- D. To established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization

Correct Answer: D

Section:

QUESTION 74

Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

- A. Senior Executives
- B. Office of the Auditor
- C. Office of the General Counsel
- D. All employees and users

Correct Answer: A

Section:

QUESTION 75

An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

- A. Management Control
- B. Technical Control
- C. Training Control
- D. Operational Control

Correct Answer: D

Section:

QUESTION 76

Which of the following illustrates an operational control process:

- A. Classifying an information system as part of a risk assessment
- B. Installing an appropriate fire suppression system in the data center
- C. Conducting an audit of the configuration management process
- D. Establishing procurement standards for cloud vendors

Correct Answer: B

Section:

QUESTION 77

With respect to the audit management process, management response serves what function?

- A. placing underperforming units on notice for failing to meet standards
- B. determining whether or not resources will be allocated to remediate a finding
- C. adding controls to ensure that proper oversight is achieved by management
- D. revealing the "root cause" of the process failure and mitigating for all internal and external units

Correct Answer: B

Section:

QUESTION 78

Which of the following are primary concerns for management with regard to assessing internal control objectives?

- A. Confidentiality, Availability, Integrity
- B. Compliance, Effectiveness, Efficiency
- C. Communication, Reliability, Cost
- D. Confidentiality, Compliance, Cost



Correct Answer: B

Section:

QUESTION 79

Which of the following are necessary to formulate responses to external audit findings?

- A. Internal Audit, Management, and Technical Staff
- B. Internal Audit, Budget Authority, Management
- C. Technical Staff, Budget Authority, Management
- D. Technical Staff, Internal Audit, Budget Authority

Correct Answer: C

Section:

QUESTION 80

The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI?

- A. Number of callers who report security issues.
- B. Number of callers who report a lack of customer service from the call center

- C. Number of successful social engineering attempts on the call center
- D. Number of callers who abandon the call before speaking with a representative

Correct Answer: C

Section:

QUESTION 81

Creating a secondary authentication process for network access would be an example of?

- A. Nonlinearities in physical security performance metrics
- B. Defense in depth cost enumerated costs
- C. System hardening and patching requirements
- D. Anti-virus for mobile devices

Correct Answer: A

Section:

QUESTION 82

Which of the following activities is the MAIN purpose of the risk assessment process?

- A. Creating an inventory of information assets
- B. Classifying and organizing information assets into meaningful groups
- C. Assigning value to each information asset
- D. Calculating the risks to which assets are exposed in their current setting

Correct Answer: D

Section:

QUESTION 83

Which of the following activities must be completed BEFORE you can calculate risk?

- A. Determining the likelihood that vulnerable systems will be attacked by specific threats
- B. Calculating the risks to which assets are exposed in their current setting
- C. Assigning a value to each information asset
- D. Assessing the relative risk facing the organization's information assets

Correct Answer: C

Section:

QUESTION 84

Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

- A. Incident response plan
- B. Business Continuity plan
- C. Disaster recovery plan
- D. Damage control plan



Correct Answer: C

Section:

QUESTION 85

Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

- A. ISO 27001
- B. ISO 27002
- C. ISO 27004
- D. ISO 27005

Correct Answer: D

Section:

QUESTION 86

Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

- A. International Organization for Standardization 27001
- B. National Institute of Standards and Technology Special Publication SP 800-12
- C. Request For Comment 2196
- D. National Institute of Standards and Technology Special Publication SP 800-26

Correct Answer: A

Section:

QUESTION 87

Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

- A. Use within an organization to formulate security requirements and objectives
- B. Implementation of business-enabling information security
- C. Use within an organization to ensure compliance with laws and regulations
- D. To enable organizations that adopt it to obtain certifications

Correct Answer: B

Section:

QUESTION 88

The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

- A. assign the responsibility to the information security team.
- B. assign the responsibility to the team responsible for the management of the controls.
- C. create operational reports on the effectiveness of the controls.
- D. perform an independent audit of the security controls.

Correct Answer: D

Section:



QUESTION 89

The effectiveness of social engineering penetration testing using phishing can be used as a Key Performance Indicator (KPI) for the effectiveness of an organization's

- A. Risk Management Program.
- B. Anti-Spam controls.
- C. Security Awareness Program.
- D. Identity and Access Management Program.

Correct Answer: C

Section:

QUESTION 90

Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

- A. Meet regulatory compliance requirements
- B. Better understand the threats and vulnerabilities affecting the environment
- C. Better understand strengths and weaknesses of the program
- D. Meet legal requirements

Correct Answer: C

Section:

QUESTION 91

The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

- A. Risk metrics
- B. Management metrics
- C. Operational metrics
- D. Compliance metrics

Correct Answer: C

Section:

QUESTION 92

When you develop your audit remediation plan what is the MOST important criteria?

- A. To remediate half of the findings before the next audit.
- B. To remediate all of the findings before the next audit.
- C. To validate that the cost of the remediation is less than the risk of the finding.
- D. To validate the remediation process with the auditor.

Correct Answer: C

Section:

QUESTION 93

Control Objectives for Information and Related Technology (COBIT) is which of the following?

- A. An Information Security audit standard
- B. An audit guideline for certifying secure systems and controls
- C. A framework for Information Technology management and governance
- D. A set of international regulations for Information Technology governance

Correct Answer: C

Section:

QUESTION 94

A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

- A. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
- B. If the findings do not impact regulatory compliance, remediate only the high and medium risk findings.
- C. If the findings impact regulatory compliance, remediate the high findings as quickly as possible.
- D. If the findings do not impact regulatory compliance, review current security controls.

Correct Answer: C

Section:

QUESTION 95

An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in severe revenue disruptions. Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

- A. The CISO
- B. Audit and Compliance
- C. The CFO
- D. The business owner

Correct Answer: D

Section:

QUESTION 96

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

- A. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
- B. A clear set of security policies and procedures that are more concept-based than controls-based
- C. A complete inventory of Information Technology assets including infrastructure, networks, applications and data
- D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Correct Answer: D

Section:

QUESTION 97

Risk appetite is typically determined by which of the following organizational functions?

- A. Security
- B. Business units
- C. Board of Directors
- D. Audit and compliance

Correct Answer: C

Section:

QUESTION 98

You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

- A. Risk averse
- B. Risk tolerant
- C. Risk conditional
- D. Risk minimal

Correct Answer: B

Section:

QUESTION 99

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

Correct Answer: B

Section:

QUESTION 100

Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

- A. Define the risk appetite
- B. Determine budget constraints
- C. Review project charters
- D. Collaborate security projects

Correct Answer: A

Section:

QUESTION 101

Which of the following is a major benefit of applying risk levels?

- A. Risk management governance becomes easier since most risks remain low once mitigated
- B. Resources are not wasted on risks that are already managed to an acceptable level



- C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
- D. Risk appetite can increase within the organization once the levels are understood

Correct Answer: B

Section:

QUESTION 102

Which of the following best summarizes the primary goal of a security program?

- A. Provide security reporting to all levels of an organization
- B. Create effective security awareness to employees
- C. Manage risk within the organization
- D. Assure regulatory compliance

Correct Answer: C

Section:

QUESTION 103

Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

- A. Risk Management
- B. Risk Assessment
- C. System Testing
- D. Vulnerability Assessment

Correct Answer: B

Section:

QUESTION 104

Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

- A. Risk Assessment
- B. Incident Response
- C. Risk Management
- D. Network Security administration

Correct Answer: C

Section:

QUESTION 105

Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

- A. System testing
- B. Risk assessment
- C. Incident response
- D. Planning



Correct Answer: A

Section:

QUESTION 106

Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

- A. Security administrators
- B. Security managers
- C. Security technicians
- D. Security analysts

Correct Answer: B

Section:

QUESTION 107

In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

- A. Distance learning/Web seminars
- B. Formal Class
- C. One-One Training
- D. Self-Study (noncomputerized)

Correct Answer: D

Section:

Explanation:

Topic 4, Information Security Core Competencies



QUESTION 108

In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:

- A. Secure the area and shut-down the computer until investigators arrive
- B. Secure the area and attempt to maintain power until investigators arrive
- C. Immediately place hard drive and other components in an anti-static bag
- D. Secure the area.

Correct Answer: B

Section:

QUESTION 109

What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

- A. Traffic Analysis
- B. Deep-Packet inspection
- C. Packet sampling
- D. Heuristic analysis

Correct Answer: B

Section:

QUESTION 110

Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

- A. Trusted and untrusted networks
- B. Type of authentication
- C. Storage encryption
- D. Log retention

Correct Answer: A

Section:

QUESTION 111

Which of the following is the MAIN security concern for public cloud computing?

- A. Unable to control physical access to the servers
- B. Unable to track log on activity
- C. Unable to run anti-virus scans
- D. Unable to patch systems as needed

Correct Answer: A

Section:

QUESTION 112

The process of identifying and classifying assets is typically included in the

- A. Threat analysis process
- B. Asset configuration management process
- C. Business Impact Analysis
- D. Disaster Recovery plan

Correct Answer: B

Section:

QUESTION 113

Which of the following is a symmetric encryption algorithm?

- A. 3DES
- B. MD5
- C. ECC
- D. RSA

Correct Answer: A

Section:

QUESTION 114



You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

- A. Execute
- B. Read
- C. Administrator
- D. Public

Correct Answer: D
Section:

QUESTION 115

As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.

- A. Covering tracks
- B. Scanning and enumeration
- C. Maintaining Access
- D. Reconnaissance
- E. Gaining Access
- F. 4, 2, 5, 3, 1
- G. 2, 5, 3, 1, 4
- H. 4, 5, 2, 3, 1
- I. 4, 3, 5, 2, 1

Correct Answer: A
Section:



QUESTION 116

What type of attack requires the least amount of technical equipment and has the highest success rate?

- A. War driving
- B. Operating system attacks
- C. Social engineering
- D. Shrink wrap attack

Correct Answer: C
Section:

QUESTION 117

Physical security measures typically include which of the following components?

- A. Physical, Technical, Operational
- B. Technical, Strong Password, Operational
- C. Operational, Biometric, Physical
- D. Strong password, Biometric, Common Access Card

Correct Answer: A

Section:

QUESTION 118

SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

- A. ' o 1=1 --
- B. /../././././
- C. "DROPTABLE USERNAME"
- D. NOPS

Correct Answer: A

Section:

QUESTION 119

An anonymity network is a series of?

- A. Covert government networks
- B. War driving maps
- C. Government networks in Tora
- D. Virtual network tunnels

Correct Answer: D

Section:

QUESTION 120

An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

- A. Shared key
- B. Asynchronous
- C. Open
- D. None

Correct Answer: A

Section:

QUESTION 121

Which wireless encryption technology makes use of temporal keys?

- A. Wireless Application Protocol (WAP)
- B. Wifi Protected Access version 2 (WPA2)
- C. Wireless Equivalence Protocol (WEP)
- D. Extensible Authentication Protocol (EAP)

Correct Answer: B

Section:



QUESTION 122

Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

- A. In-line hardware keyloggers don't require physical access
- B. In-line hardware keyloggers don't comply to industry regulations
- C. In-line hardware keyloggers are undetectable by software
- D. In-line hardware keyloggers are relatively inexpensive

Correct Answer: C

Section:

QUESTION 123

The process of creating a system which divides documents based on their security level to manage access to private data is known as

- A. security coding
- B. data security system
- C. data classification
- D. privacy protection

Correct Answer: C

Section:

QUESTION 124

A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

- A. non-repudiation
- B. conflict resolution
- C. strong authentication
- D. digital rights management

Correct Answer: A

Section:

QUESTION 125

When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?

- A. SaaS provider's website certifications and representations (certs and reps)
- B. SOC-2 Report
- C. Metasploit Audit Report
- D. Statement from SaaS provider attesting their ability to secure your data

Correct Answer: B

Section:

Explanation:

Reference: <https://www.threatstack.com/blog/how-saas-companies-can-build-a-complianceroadmap>

QUESTION 126

As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.

Which is the BEST type of risk that defines this event?

- A. Compliance Risk
- B. Reputation Risk
- C. Operational Risk
- D. Strategic Risk

Correct Answer: B

Section:

QUESTION 127

What is a Statement of Objectives (SOA)?

- A. A section of a contract that defines tasks to be performed under said contract
- B. An outline of what the military will do during war
- C. A document that outlines specific desired outcomes as part of a request for proposal
- D. Business guidance provided by the CEO

Correct Answer: A

Section:

QUESTION 128

The process for identifying, collecting, and producing digital information in support of legal proceedings is called

- A. chain of custody.
- B. electronic discovery.
- C. evidence tampering.
- D. electronic review.

Correct Answer: B

Section:

QUESTION 129

Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?

- A. Configure logging on each access point
- B. Install a firewall software on each wireless access point.
- C. Provide IP and MAC address
- D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.

Correct Answer: C

Section:

QUESTION 130

One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

- A. Your public key
- B. The recipient's private key
- C. The recipient's public key
- D. Certificate authority key

Correct Answer: C

Section:

QUESTION 131

Which of the following is a countermeasure to prevent unauthorized database access from web applications?

- A. Session encryption
- B. Removing all stored procedures
- C. Input sanitization
- D. Library control

Correct Answer: C

Section:

QUESTION 132

Which of the following statements about Encapsulating Security Payload (ESP) is true?

- A. It is an IPSec protocol.
- B. It is a text-based communication protocol.
- C. It uses TCP port 22 as the default port and operates at the application layer.
- D. It uses UDP port 22

Correct Answer: A

Section:

QUESTION 133

The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

- A. Well established and defined digital forensics process
- B. Establishing Enterprise-owned Botnets for preemptive attacks
- C. Be able to retaliate under the framework of Active Defense
- D. Collaboration with law enforcement

Correct Answer: A

Section:

QUESTION 134

Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?



- A. Comprehensive Log-Files from all servers and network devices affected during the attack
- B. Fully trained network forensic experts to analyze all data right after the attack
- C. Uninterrupted Chain of Custody
- D. Expert forensics witness

Correct Answer: C

Section:

QUESTION 135

The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

- A. The need to change accounting periods on a regular basis.
- B. The requirement to post entries for a closed accounting period.
- C. The need to create and modify the chart of accounts and its allocations.
- D. The lack of policies and procedures for the proper segregation of duties.

Correct Answer: D

Section:

QUESTION 136

Which of the following is a common technology for visual monitoring?

- A. Closed circuit television
- B. Open circuit television
- C. Blocked video
- D. Local video

Correct Answer: A

Section:

Explanation:

Reference: <https://www.ifsecglobal.com/video-surveillance/role-cctv-cameras-public-privacyprotection/>

QUESTION 137

Which of the following is an accurate statement regarding capital expenses?

- A. They are easily reduced through the elimination of usage, such as reducing power for lighting of work areas during off-hours
- B. Capital expenses can never be replaced by operational expenses
- C. Capital expenses are typically long-term investments with value being realized through their use
- D. The organization is typically able to regain the initial cost by selling this type of asset

Correct Answer: A

Section:

QUESTION 138

A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?



- A. The internal accounting department
- B. The Chief Financial Officer (CFO)
- C. The external financial audit service
- D. The managers of the accounts payables and accounts receivables teams

Correct Answer: D

Section:

QUESTION 139

A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

- A. Poorly configured firewalls
- B. Malware
- C. Advanced Persistent Threat (APT)
- D. An insider

Correct Answer: D

Section:

QUESTION 140

Which of the following defines the boundaries and scope of a risk assessment?

- A. The risk assessment schedule
- B. The risk assessment framework
- C. The risk assessment charter
- D. The assessment context

Correct Answer: B

Section:

Explanation:

Reference: <https://cfocussoftware.com/risk-management-framework/know-your-boundary/>

QUESTION 141

Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

- A. They need to use Nessus.
- B. They can implement Wireshark.
- C. Snort is the best tool for their situation.
- D. They could use Tripwire.

Correct Answer: C

Section:

Explanation:



Reference: <https://searchnetworking.techtarget.com/definition/Snort>

QUESTION 142

Which of the following is true regarding expenditures?

- A. Capital expenditures are never taxable
- B. Operating expenditures are for acquiring assets, capital expenditures are for support costs of that asset
- C. Capital expenditures are used to define depreciation tables of intangible assets
- D. Capital expenditures are for acquiring assets, whereas operating expenditures are for support costs of that asset

Correct Answer: D

Section:

QUESTION 143

At what level of governance are individual projects monitored and managed?

- A. Program
- B. Milestone
- C. Enterprise
- D. Portfolio

Correct Answer: D

Section:

QUESTION 144

A digital signature addresses which of the following concerns?

- A. Message alteration
- B. Message copying
- C. Message theft
- D. Unauthorized reading

Correct Answer: A

Section:

Explanation:

Reference: <https://www.entrust.com/resources/certificate-solutions/learn/digital-signatures>

QUESTION 145

What are the three stages of an identity and access management system?

- A. Authentication, Authorize, Validation
- B. Provision, Administration, Enforcement
- C. Administration, Validation, Protect
- D. Provision, Administration, Authentication

Correct Answer: A

Section:



Explanation:

Reference: <https://digitalguardian.com/blog/what-identity-and-access-management-iam>

QUESTION 146

During the last decade, what trend has caused the MOST serious issues in relation to physical security?

- A. Data is more portable due to the increased use of smartphones and tablets
- B. The move from centralized computing to decentralized computing
- C. Camera systems have become more economical and expanded in their use
- D. The internet of Things allows easy compromise of cloud-based systems

Correct Answer: A

Section:

QUESTION 147

Which of the following is the MOST important reason for performing assessments of the security portfolio?

- A. To assure that the portfolio is aligned to the needs of the broader organization
- B. To create executive support of the portfolio
- C. To discover new technologies and processes for implementation within the portfolio
- D. To provide independent 3rd party reviews of security effectiveness

Correct Answer: A

Section:

QUESTION 148

Which of the following terms is used to describe countermeasures implemented to minimize risks to physical property, information, and computing systems?

- A. Security frameworks
- B. Security policies
- C. Security awareness
- D. Security controls

Correct Answer: D

Section:

Explanation:

Reference: <https://www.ibm.com/cloud/learn/security-controls>

QUESTION 149

Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

- A. Identification
- B. Authorization
- C. Authentication
- D. Accountability

Correct Answer: B



Section:

QUESTION 150

As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

- A. Gigamon
- B. Intrusion Prevention System
- C. Port Security
- D. Anti-virus

Correct Answer: B

Section:

Explanation:

Reference: <https://searchsecurity.techtarget.com/definition/intrusion-prevention>

QUESTION 151

Michael starts a new job and discovers that he has unnecessary access to a variety of systems. Which of the following best describes the problem he has encountered?

- A. Rights collision
- B. Excessive privileges
- C. Privilege creep
- D. Least privileges

Correct Answer: B

Section:

QUESTION 152

Which of the following best describes the sensors designed to project and detect a light beam across an area?

- A. Smoke
- B. Thermal
- C. Air-aspirating
- D. Photo electric

Correct Answer: D

Section:

Explanation:

Reference: https://en.wikipedia.org/wiki/Photoelectric_sensor

QUESTION 153

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

- A. File Transfer Protocol (FTP)
- B. Virtual Local Area Network (VLAN)
- C. Simple Mail Transfer Protocol



D. Virtual Private Network (VPN)

Correct Answer: D

Section:

Explanation:

Reference: <https://searchnetworking.techtarget.com/definition/virtual-private-network>

QUESTION 154

As the CISO, you have been tasked with the execution of the company's key management program.

You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

- A. Dual Control
- B. Separation of Duties
- C. Split Knowledge
- D. Least Privilege

Correct Answer: A

Section:

Explanation:

Reference: <https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management>

QUESTION 155

What is one key difference between Capital expenditures and Operating expenditures?

- A. Operating expense cannot be written off while Capital expense can
- B. Operating expenses can be depreciated over time and Capital expenses cannot
- C. Capital expenses cannot include salaries and Operating expenses can
- D. Capital expenditures allow for the cost to be depreciated over time and Operating does not



Correct Answer: C

Section:

QUESTION 156

Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

- A. Segmentation controls.
- B. Shadow applications.
- C. Deception technology.
- D. Vulnerability management.

Correct Answer: B

Section:

QUESTION 157

Which of the following is an accurate description of a balance sheet?

- A. The percentage of earnings that are retained by the organization for reinvestment in the business

- B. The details of expenses and revenue over a long period of time
- C. A summarized statement of all assets and liabilities at a specific point in time
- D. A review of regulations and requirements impacting the business from a financial perspective

Correct Answer: C

Section:

QUESTION 158

A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

- A. Moderate investment
- B. Passive monitoring
- C. Integrated security controls
- D. Dynamic deception

Correct Answer: D

Section:

QUESTION 159

What is the difference between encryption and tokenization?

- A. Tokenization combined with hashing is always better than encryption
- B. Encryption can be mathematically reversed to provide the original information
- C. The token contains the all original information
- D. Tokenization can be mathematically reversed to provide the original information



Correct Answer: B

Section:

Explanation:

Reference: http://library.ahima.org/doc?oid=104090#.X_dwWoIR3eQ

QUESTION 160

Which of the following information would MOST likely be reported at the board-level within an organization?

- A. System scanning trends and results as they pertain to insider and external threat sources
- B. The capabilities of a security program in terms of staffing support
- C. Significant risks and security incidents that have been discovered since the last assembly of the membership
- D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

Correct Answer: C

Section:

QUESTION 161

Which technology can provide a computing environment without requiring a dedicated hardware backend?

- A. Mainframe server

- B. Virtual Desktop
- C. Thin client
- D. Virtual Local Area Network

Correct Answer: B

Section:

QUESTION 162

What process defines the framework of rules and practices by which a board of directors ensure accountability, fairness and transparency in an organization's relationship with its shareholders?

- A. Internal Audit
- B. Corporate governance
- C. Risk Oversight
- D. Key Performance Indicators

Correct Answer: B

Section:

Explanation:

Reference: <https://www.igi-global.com/dictionary/corporate-governance/5957>

QUESTION 163

As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

- A. Recovery Point Objective (RPO)
- B. Disaster Recovery Plan
- C. Recovery Time Objective (RTO)
- D. Business Continuity Plan



Correct Answer: D

Section:

Explanation:

Reference: <https://www.resolver.com/resource/bcdr-metrics-that-matter/>

QUESTION 164

What are the three hierarchically related aspects of strategic planning and in which order should they be done?

- A. 1) Information technology strategic planning, 2) Enterprise strategic planning, 3) Cybersecurity or information security strategic planning
- B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3) Information technology strategic planning
- C. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
- D. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3) Information technology strategic planning

Correct Answer: D

Section:

QUESTION 165

Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?

- A. ITIL
- B. Privacy Act
- C. Sarbanes Oxley
- D. PCI-DSS

Correct Answer: B

Section:

QUESTION 166

Which of the following would negatively impact a log analysis of a multinational organization?

- A. Centralized log management
- B. Encrypted log files in transit
- C. Each node set to local time
- D. Log aggregation agent each node

Correct Answer: D

Section:

Explanation:

Topic 6, Misc. Questions

QUESTION 167

Which of the following statements below regarding Key Performance indicators (KPIs) are true?

- A. Development of KPI's are most useful when done independently
- B. They are a strictly quantitative measure of success
- C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
- D. They are a strictly qualitative measure of success

Correct Answer: A

Section:

Explanation:

Reference: <https://kpi.org/KPI-Basics/KPI-Development>

QUESTION 168

When information security falls under the Chief Information Officer (CIO), what is their MOST essential role?

- A. Oversees the organization's day-to-day operations, creating the policies and strategies that govern operations
- B. Enlisting support from key executives the information security program budget and policies
- C. Charged with developing and implementing policies designed to protect employees and customers' data from unauthorized access
- D. Responsible for the success or failure of the IT organization and setting strategic direction

Correct Answer: D

Section:

Explanation:

Reference: <https://www.investopedia.com/terms/c/cio.asp>



QUESTION 169

APLU Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk.

Which metric would meet the requirement?

- A. Number of times third parties access critical information systems
- B. Number of systems with known vulnerabilities
- C. Number of users with elevated privileges
- D. Number of websites with weak or misconfigured certificates

Correct Answer: C

Section:

QUESTION 170

An organization recently acquired a Data Loss Prevention (DLP) solution, and two months after the implementation, it was found that sensitive data was posted to numerous Dark Web sites. The DLP application was checked, and there are no apparent malfunctions and no errors.

What is the MOST likely reason why the sensitive data was posted?

- A. The DLP Solution was not integrated with mobile device anti-malware
- B. Data classification was not properly performed on the assets
- C. The sensitive data was not encrypted while at rest
- D. A risk assessment was not performed after purchasing the DLP solution

Correct Answer: D

Section:

**QUESTION 171**

The main purpose of the SOC is:

- A. An organization which provides Tier 1 support for technology issues and provides escalation when needed
- B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities
- C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation
- D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

Correct Answer: C

Section:

Explanation:

Reference: <https://www.eccouncil.org/what-is-soc/>

QUESTION 172

When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

- A. This makes sure the files you exchange aren't unnecessarily flagged by the Data Loss Prevention (DLP) system
- B. Contracting rules typically require you to have conversations with two or more groups
- C. Discussing decisions with a very large group of people always provides a better outcome
- D. It helps to avoid regulatory or internal compliance issues

Correct Answer: D

Section:

Explanation:

Reference: <https://www.eccouncil.org/wp-content/uploads/2016/07/NICE-2.0-and-EC-Council-Cert-Mapping.pdf>

QUESTION 173

A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

- A. Public cloud
- B. Private cloud
- C. Community cloud
- D. Hybrid cloud

Correct Answer: D

Section:

Explanation:

Reference: <https://www.datacenters.com/services/cloudservices#:~:text=Hybrid%20clouds%20combine%20public%20and,flexibility%20and%20more%20deployment%20options>

