712-50.187q

Number: 712-50
Passing Score: 800
Time Limit: 120 min

712-50

EC-Council Certified CISO (CCISO)

Exam A

QUESTION 1
When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

A. Eradication
B. Escalation
C. Containment
D. Recovery

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
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. There is no relationship between the two.
D. 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.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 3

Who in the organization determines access to information?

A. Compliance officer
B. Legal department
C. Data Owner
D. Information security officer

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

A. Compliance with local privacy regulations
B. An independent Governance, Risk and Compliance organization
C. Support Legal and HR teams
D. Alignment of security goals with business goals

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
The FIRST step in establishing a security governance program is to?

A. Obtain senior level sponsorship B.
Conduct a workshop for all end users.
C. Conduct a risk assessment.
D. Prepare a security budget.
Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 6

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy.

This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?

A. Lack of a formal risk management policy
B. Lack of a formal security policy governance process
C. Lack of normal definition of roles and responsibilities

D. Lack of a formal security awareness program

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11

Regulatory requirements typically force organizations to implement ____________.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12

From an information security perspective, information that no longer supports the main purpose of the business should be:

A. protected under the information classification policy
B. analyzed under the data ownership policy
C. assessed by a business impact analysis.
D. analyzed under the retention policy.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13

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. National Institute for Standards and technology (NIST) standard
C. International Organization for Standardization (ISO) standards
D. Payment Card Industry Data Security Standards (PCI-DSS)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14

One of the MAIN goals of a Business Continuity Plan is to_______________.

A. Ensure all infrastructure and applications are available in the event of a disaster
B. Assign responsibilities to the technical teams responsible for the recovery of all data
C. Provide step by step plans to recover business processes in the event of a disaster
D. Allow all technical first-responders to understand their roles in the event of a disaster.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15

An organization's Information Security Policy is of MOST importance because_____________.

A. It defines a process to meet compliance requirements
B. It establishes a framework to protect confidential information
C. It communicates management’s commitment to protecting information resources

D. It is formally acknowledged by all employees and vendors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 16

The alerting, monitoring and life-cycle management of security related events is typically handled by the_________________.

A. risk management process
B. risk assessment process
C. governance, risk, and compliance tools
D. security threat and vulnerability management process

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17

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: (none)
Explanation

Explanation/Reference:

QUESTION 18

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

A. Threat identification
B. Risk treatment
C. Risk monitoring
D. Risk tolerance

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

Which of the following is a benefit of information security governance?

A. Direct involvement of senior management in developing control processes

B. Reduction of the potential for civil and legal liability

C. Questioning the trust in vendor relationships

D. Increasing the risk of decisions based on incomplete management information

Correct Answer: B

Section: (none)

Explanation

Explanation/Reference:

QUESTION 21

Developing effective security controls is a balance between:

A. Technology and Vendor Management

B. Operations and Regulations

C. Risk Management and Operations

D. Corporate Culture and Job Expectations

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 22

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 Compromise

B. Due process

C. Due Care
D. Due Protection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
Which of the following is considered the MOST effective tool against social engineering?

A. Effective Security Vulnerability Management Program
B. Anti-malware tools
C. Effective Security awareness program
D. Anti-phishing tools

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
When managing the security architecture for your company you must consider:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 25

The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.

B. Establishing incident response programs.
C. Establishing strategic alignment with business continuity requirements.
D. Identifying and implementing the best security solutions.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27

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

A. They are subjective and can be completed more quickly
B. They are objective and express risk / cost in approximates

C. They are subjective and can express risk / cost real numbers
D. They are objective and can express risk / cost in real numbers

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 28
Which of the following most commonly falls within the scope of an information security governance steering committee?

A. Vetting information security policies
B. Approving access to critical financial systems
C. Interviewing candidates for information security specialist positions
D. Developing content for security awareness programs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
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. Industry certifications, technical knowledge and program management skills
B. Multiple references, strong background check and industry certifications
C. Multiple certifications, strong technical capabilities and lengthy resume
D. College degree, audit capabilities and complex project management

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

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

A. Ensure that security policies and procedures have been vetted and approved.
B. Review all past audit and compliance reports.
C. Include a mix of members from different departments and staff levels.
D. Review all past audit and compliance reports.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

Risk that remains after risk mitigation is known as_____________.

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

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. Payment Card Industry Data Security Standards (PCI-DSS)

B. International Organization for Standardizations – 27005 (ISO-27005)
C. International Organization for Standardizations – 27004 (ISO-27004)
D. Control Objectives for Information Technology (COBIT)

Correct Answer: C
Section: (none)

QUESTION 33
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 variety of technologies deployed in the infrastructure.
B. When it results in an overall lower cost of operating the security program.
C. When there is a need to develop a more unified incident response capability.
D. When the enterprise is made up of many business units with diverse business activities, risks profiles and regulatory requirements.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 34
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights.

Which of the following would be the MOST concerning?

A. Failure to notify police of an attempted intrusion
B. Lack of reporting of a successful denial of service attack on the network.
C. Lack of notification to the public of disclosure of confidential information
D. Lack of notification to the public of disclosure of confidential information

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 35
Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?
A. Value of the asset multiplied by the loss expectancy
B. Replacement cost multiplied by the single loss expectancy
C. Single loss expectancy multiplied by the annual rate of occurrence
D. Total loss expectancy multiplied by the total loss frequency

Explanation

Explanation/Reference:
Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 36
The Information Security Management program MUST protect:

A. Against distributed denial of service attacks
B. Intellectual property released into the public domain C. all organizational assets
D. critical business processes and/or revenue streams

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 37
Dataflow diagrams are used by IT auditors to:

A. Graphically summarize data paths and storage processes.
B. Order data hierarchically
C. Highlight high-level data definitions
D. Portray step-by-step details of data generation.

Correct Answer: A
Section: (none)
QUESTION 38
When measuring the effectiveness of an Information Security Management System which one of the following would be MOST LIKELY used as a metric framework?

A. ISO 27001
B. ISO 27004
C. PRINCE2
D. ITILv3

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
The purpose of NIST SP 800-53 as part of the NIST System Certification and Accreditation Project is to establish a set of standardized, minimum security controls for IT systems addressing low, moderate, and high levels of concern for:

A. Integrity and Availability
B. Assurance, Compliance and Availability
C. International Compliance
D. Confidentiality, Integrity and Availability

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40
An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security___________.

A. Technical control
B. Management control
C. Procedural control
D. Administrative control

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 41

Explanation

Explanation/Reference:
Information security policies should be reviewed ____________________.

A. by the internal audit semiannually
B. by the CISO when new systems are brought online
C. by the Incident Response team after an audit
D. by stakeholders at least annually

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 42
Risk is defined as:

A. Quantitative plus qualitative impact
B. Asset loss times likelihood of event
C. Advisory plus capability plus vulnerability
D. Threat times vulnerability divided by control

Correct Answer: D
Section: (none)
QUESTION 43
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

A. The organization uses exclusively a qualitative process to measure risk
B. The organization's risk tolerance is low
C. The organization uses exclusively a quantitative process to measure risk
D. The organization's risk tolerance is high

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 44

The regular review of a firewall ruleset is considered a ______________________.

A. Procedural control
B. Organization control
C. Management control
D. Technical control

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 45

The exposure factor of a threat to your organization is defined by?

A. Annual loss expectancy minus current cost of controls
B. Percentage of loss experienced due to a realized threat event
C. Asset value times exposure factor
D. Annual rate of occurrence

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 46

The Information Security Governance program MUST:

A. integrate with other organizational governance processes
B. show a return on investment for the organization
C. integrate with other organizational governance processes
D. support user choice for Bring Your Own Device (BYOD)

Correct Answer: C

Explanation

Explanation/Reference:
Section: (none) Explanation

Explanation/Reference:

QUESTION 47
You have recently drafted a revised information security policy. From whom should you seek endorsement in order to have the GREATEST chance for adoption and implementation throughout the entire organization?

A. Chief Executive Officer
B. Chief Information Officer
C. Chief Information Security Officer
D. Chief Information Officer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 48

Which of the following is a benefit of a risk-based approach to audit planning?

A. Resources are allocated to the areas of the highest concern
B. Scheduling may be performed months in advance
C. Budgets are more likely to be met by the IT audit staff
D. Staff will be exposed to a variety of technologies

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 49

Which of the following are the MOST important factors for proactively determining system vulnerabilities?

A. Subscribe to vendor mailing list to get notification of system vulnerabilities
B. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
C. Conduct security testing, vulnerability scanning, and penetration testing
D. Deploy Intrusion Detection System (IDS) and install anti-virus on systems

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 50

When choosing a risk mitigation method what is the MOST important factor?

A. Approval from the board of directors
B. Metrics of mitigation method success
C. Cost of the mitigation is less than a risk
D. Mitigation method complies with PCI regulations

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
Payment Card Industry (PCI) compliance requirements are based on what criteria?

A. The size of the organization processing credit card data
B. The types of cardholder data retained
C. The duration card holder data is retained
D. The number of transactions performed per year by an organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
What role should the CISO play in properly scoping a PCI environment?

A. Complete the self-assessment questionnaire and work with an Approved Scanning Vendor (ASV) to determine scope
B. Work with a Qualified Security Assessor (QSA) to determine the scope of the PCI environment
C. Validate the business units' suggestions as to what should be included in the scoping process
D. Ensure internal scope validation is completed and that an assessment has been done to discover all credit card data

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:
QUESTION 53
Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

A. Systems logs

B. Hardware error reports
C. Availability reports
D. Utilization reports

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 54
An organization information security policy serves to___________________.

A. define security configurations for systems
B. establish budgetary input in order to meet compliance requirements
C. establish acceptable systems and user behavior
D. define relationship with external law enforcement agencies

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 55
An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator.

The most appropriate course of action for the IT auditor is to:

A. Review the system log for each of the late night shifts to determine whether any irregular actions occurred.
B. Inform senior management of the risk involved.
C. Develop a computer assisted audit technique to detect instances of abuses of the arrangement.
D. Agree to work with the security officer on these shifts as a form of preventative.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57

IT control objectives are useful to IT auditors as they provide the basis for understanding the:

A. The audit control checklist
B. Technique for securing information
C. Desired results or purpose of implementing specific control procedures.
D. Security policy

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:
QUESTION 58

Which of the following activities results in change requests?

A. Corrective actions
B. Defect repair
C. Preventive actions
D. Inspection

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 59
What is the MAIN reason for conflicts between Information Technology and Information Security programs?

A. The effective implementation of security controls can be viewed as an inhibitor to rapid Information technology implementations.
B. Technology Governance is focused on process risks whereas Security Governance is focused on business risk.
C. Technology governance defines technology policies and standards while security governance does not.
D. Security governance defines technology best practices and Information Technology governance does not.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60
Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How the security operations team will behave to reported incidents
B. How vulnerabilities can potentially be exploited in systems that impact the organization
C. How the firewall and other security devices are configured to prevent attacks
D. How the incident management team prepares to handle an attack
Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 61
Who is responsible for securing networks during a security incident?

A. Security Operations Center (SOC)

B. Chief Information Security Officer (CISO)
C. Disaster Recovery (DR) manager
D. Incident response Team (IRT)

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 62
What is the BEST way to achieve on-going compliance monitoring in an organization?

A. Outsource compliance to a 3rd party vendor and let them manage the program.
B. Have Compliance Direct Information Security to fix issues after the auditor’s report.
C. Only check compliance right before the auditors are scheduled to arrive onsite.
D. Have Compliance and Information Security partner to correct issues as they arise.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 63
The success of the Chief Information Security Officer is MOST dependent upon:
A. following the recommendations of consultants and contractors
B. raising awareness of security issues with end users
C. favorable audit findings
D. development of relationships with organization executives

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 64

During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

A. Identify and assess the risk assessment process used by management.
B. Identify and evaluate existing controls.
C. Identify information assets and the underlying systems.
D. Disclose the threats and impacts to management.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 65

Which of the following is a fundamental component of an audit record?

A. Originating IP-Address
B. Date and time of the event
C. Failure of the event
D. Authentication type

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66

What is the main purpose of the Incident Response Team?

A. Communicate details of information security incidents
B. Create effective policies detailing program activities
C. Ensure efficient recovery and reinstate repaired systems
D. Provide current employee awareness programs

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 67
Risk appetite directly affects what part of a vulnerability management program?

A. Scope
B. Schedule
C. Staff
D. Scan tools

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 68
Creating a secondary authentication process for network access would be an example of?

A. An administrator with too much time on their hands
B. Supporting the concept of layered security
C. Network segmentation
D. Putting undue time commitment on the system administrator

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 69
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

A. Decide how to manage risk

B. Define Information Security Policy
C. Identify threats, risks, impacts and vulnerabilities
D. Define the budget of the Information Security Management System

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 70
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

A. Human Resources and Budget
B. Audit and Legal
C. Budget and Compliance
D. Legal and Human Resources

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:
QUESTION 71
The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

A. Technical control
B. Management control
C. Procedural control
D. Organization control

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72

Which of the following is a term related to risk management that represents the estimated frequency at which a threat is expected to transpire?

A. Temporal Probability (TP)
B. Annualized Rate of Occurrence (ARO)
C. Single Loss Expectancy (SLE)
D. Exposure Factor (EF)

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure.

What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

A. Decrease the vulnerabilities within the scan tool settings
B. Scan a representative sample of systems
C. Filter the scan output so only pertinent data is analyzed
D. Perform the scans only during off-business hours

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 74
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

A. Conduct a Disaster Recovery (RD) exercise every year to test the plan
B. Conduct periodic tabletop exercises to refine the BC plan
C. Test every three years to ensure that things work as planned

D. Outsource the creation and execution of the BC plan to a third party vendor

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 75
According to the National Institute of Standards and Technology (NIST) SP 800-40, which of the following considerations are MOST important when creating a vulnerability management program?

A. Susceptibility to attack, expected duration of attack, and mitigation availability
B. Attack vectors, controls cost, and investigation staffing needs
C. Susceptibility to attack, mitigation response time, and cost
D. Vulnerability exploitation, attack recovery, and mean time to repair

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it___________

A. In-lie and turn on alert mode to stop malicious traffic.

B. In promiscuous mode and block malicious traffic.
C. In promiscuous mode and only detect malicious traffic.
D. In-line and turn on blocking mode to stop malicious traffic.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

A. Vulnerability
B. Threat
C. Exploitation
D. Attack vector

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
QUESTION 78
How often should an environment be monitored for cyber threats, risks, and exposures?

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

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 79
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 servers
C. Only critical and high vulnerabilities on servers and desktops
D. All vulnerabilities that impact important production servers

Correct Answer: B **Section:**
(none) Explanation

Explanation/Reference:

QUESTION 80
An international organization is planning a project to implement encryption technologies to protect company confidential information. This organization has data centers on three continents.

Which of the following would be considered a MAJOR constraint for the project?

A. Compliance to local hiring laws
B. Encryption import/export regulations
C. Local customer privacy laws
D. Time zone differences

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 81
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. Review the recommendations and follow up to see if audit implemented the changes
B. Meet with audit team to determine a timeline for corrections
C. Have internal audit conduct another audit to see what has changed.
D. Contract with an external audit company to conduct an unbiased audit

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 82
The risk found after a control has been fully implemented is called:

A. Total Risk
B. Transferred Risk
C. Residual Risk
D. Post Implementation Risk

Correct Answer: C **Section:**
(none) Explanation

Explanation/Reference:

QUESTION 83
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-Select-Implement-Evaluate
C. Plan-Do-Check-Act
D. SCORE (Security Consensus Operational Readiness Evaluation)

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 84
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 organization has purchased cyber insurance
B. The risk tolerance of the organization permits this risk
C. The CIO of the organization disagrees with the finding
D. The auditors have not followed proper auditing processes

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 85
When you develop your audit remediation plan what is the MOST important criteria?
A. To validate the remediation process with the auditor.
B. To validate that the cost of the remediation is less than risk of the finding.
C. To remediate half of the findings before the next audit.
D. To remediate all of the findings before the next audit.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 86
To have accurate and effective information security policies how often should the CISO review the organization policies?

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

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 87
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. Reputational Impact, Financial impact, and Risk of Compromise
D. Risk transfer, reputational Impact, and Consequences of Compromise

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
When managing the critical path of an IT security project, which of the following is MOST important?

A. Knowing who all the stakeholders are.
B. Knowing the milestones and timelines of deliverables.
C. Knowing the people on the data center team.
D. Knowing the threats to the organization.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 89
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, anti-virus console, IDS, syslog
C. Firewall, exchange, web server, intrusion detection system (IDS)
D. IDS, syslog, router, switches

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 90
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 do not impact regulatory compliance, remediate only the high and medium risk findings.
B. If the findings do not impact regulatory compliance, review current security controls.
C. If the findings impact regulatory compliance, try to apply remediation that will address the most findings for the least cost.
D. if the findings impact regulatory compliance, remediate the high findings as quickly as possible.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 91
At which point should the identity access management team be notified of the termination of an employee?

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

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 92
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. Office of the General Counsel
B. Office of the Auditor
C. Senior Executives
D. All employee and users

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 93
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

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

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 94
With respect to the audit management process, management response serves what function?

A. revealing the “root cause” of the process failure and mitigating for all internal and external units
B. adding controls to ensure that proper oversight is achieved by management

C. determining whether or not resources will be allocated to remediate a finding
D. placing underperforming units on notice for failing to meet standards

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 95
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 audit findings is incorrect
B. The asset is more expensive than the remediation
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: (none) Explanation

Explanation/Reference:

QUESTION 96
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
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, configuration adjustment, Software Removal
B. Install software patch, operate system, Maintain system
C. Discover software, Remove affected software, Apply software patch
D. Software removal, install software patch, maintain system

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 98
Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
Which represents PROPER separation of duties in the corporate environment?

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

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 100
When working in the Payment Card Industry (PCI), how often should security logs be review to comply with the standards?

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

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 101
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. perform an independent audit of the security controls
D. create operational reports on the effectiveness of the controls.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
The ultimate goal of an IT security projects is:

A. Support business requirements
B. Implement information security policies
C. Increase stock value
D. Complete security

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 103
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 and length of planned outages
B. Number of change orders processed
C. Number of change orders rejected
D. Number of unplanned outages

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
You have implemented the new controls. What is the next step?

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

Correct Answer: B

Section: (none) Explanation

Explanation/Reference:

QUESTION 105

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

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

Correct Answer: B

Section: (none) Explanation

Explanation/Reference:

QUESTION 106

Which of the following illustrates an operational control process:

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

Correct Answer: C

Section: (none)

Explanation

Explanation/Reference:

QUESTION 107

A person in your security team calls you at night and informs you that one of your web applications is potentially under attack from a cross-site scripting vulnerability.

What do you do?

A. tell him to shut down the server
B. tell him to call the police
C. tell him to invoke the incident response process
D. tell him to analyze the problem, preserve the evidence and provide a full analysis and report.

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
Which of the following are necessary to formulate responses to external audit findings?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

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

Correct Answer: A **Section: (none) Explanation**

Explanation/Reference:

QUESTION 110

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: (none) Explanation

Explanation/Reference:

QUESTION 111

Acme Inc. has engaged a third party vendor to provide 99.999% up-time for their online web presence and had them contractually agree to this service level agreement.

What type of risk tolerance is Acme exhibiting?

A. medium-high risk-tolerance
B. low risk-tolerance
C. high risk-tolerance
D. moderate risk-tolerance

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 112

Your incident response plan should include which of the following?

A. Procedures for classification

B. Procedures for charge-back
C. Procedures for reclamation
D. Procedures for litigation

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 113
To get an Information Security project back on schedule, which of the following will provide the MOST help?

A. Upper management support
B. More frequent project milestone meetings
C. Stakeholder support
D. None
E. Extend work hours

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 114
You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll.

Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff?

A. Employ an assumption of breach protocol and defend only essential information resources.
B. Deploy a SEIM solution and have current staff review incidents first in the morning
C. Configure your syslog to send SMS messages to current staff when target events are triggered.
D. Contract with a managed security provider and have current staff on recall for incident response

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 115

A department within your company has proposed a third party vendor solution to address an urgent, critical business need. As the CISO you have been asked to accelerate screening of their security control claims.

Which of the following vendor provided documents is BEST to make your decision?

A. Vendor provided reference from an existing reputable client detailing their implementation
B. Vendor's client list of reputable organizations currently using their solution
C. Vendor provided internal risk assessment and security control documentation
D. Vendor provided attestation of the detailed security controls from a reputable accounting firm

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 116

A severe security threat has been detected on your corporate network. As CISO you quickly assemble key members of the Information Technology team and business operations to determine a modification to security controls in response to the threat.

This is an example of:

A. Change management
B. Thought leadership
C. Business continuity planning
D. Security Incident Response

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:
QUESTION 117

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

A. Create collaborative risk management approaches within the organization
B. Perform increased audits of security processes and procedures
C. Provide clear communication of security requirements throughout the organization
D. Demonstrate executive support with written mandates for security policy adherence

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 118
When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization.

Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

A. Download security tools from a trusted source and deploy to production network
B. Download open source security tools from a trusted site, test, and then deploy on production network
C. Download trial versions of commercially available security tools and deploy on your production network
D. Download open source security tools and deploy them on your production network

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 119
How often should the SSAE16 report of your vendors be reviewed?

A. Quarterly
B. Semi-annually
C. Bi-annually
D. Annually

Correct Answer: D **Section: (none) Explanation**

Explanation/Reference:

QUESTION 120

Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

A. More frequent project milestone meetings
B. Involve internal audit
C. Upper management support
D. More training of staff members

Correct Answer: C **Section: (none) Explanation**

Explanation/Reference:

QUESTION 121

The organization does not have the time to remediate the vulnerability; however it is critical to release the application.

Which of the following needs to be further evaluated to help mitigate the risks?

A. Provide security testing tools
B. Provide developer security training
C. Deploy Intrusion Detection Systems
D. Implement Compensating Controls

Correct Answer: D
Section: (none)
Explanation
Explanation/Reference:

QUESTION 122

Your company has a “no right to privacy” notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee’s email account.

What should you do?

A. Deny the request citing national privacy laws
B. None
C. Grant her access, the employee has been adequately warned through the AUP.
D. Assist her with the request, but only after her supervisor signs off on the action.
E. Reset the employee's password and give it to the supervisor.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 123
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 managers
B. Security analysts
C. Security technicians
D. Security administrators

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 124
Which of the following is a major benefit of applying risk levels?

A. Resources are not wasted on risks that are already managed to an acceptable level
B. Risk appetite increase within the organization once the levels are understood
C. Risk budgets are more easily managed due to fewer due to fewer identified risks as a result of using a methodology
D. Risk management governance becomes easier since most risks remain low once mitigated

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 125
Which business stakeholder is accountable for the integrity of a new information system?

A. Compliance Officer
B. CISO
C. Project manager
D. Board of directors

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 126
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization.

Which of the following principles does this best demonstrate?

A. Proper budget management
B. Effective use of existing technologies
C. Alignment with the business
D. Leveraging existing implementations
Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 127
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

A. Risk Assessment
B. Risk Management

C. Vulnerability Assessment
D. System Testing

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
Which of the following information may be found in table top exercises for incident response?

A. Real-time to remediate
B. Process improvements
C. Security budget augmentation
D. Security control selection

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 129
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?

A. Type of data contained in the process/system

B. Type of encryption required for the data once it is at rest
C. Type of computer the data is processed on
D. Type of connection/protocol used to transfer the data

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 130
A stakeholder is a person or group:

A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
B. That will ultimately use the system.
C. That has budget authority.
D. Vested in the success and/or failure of a project or initiative and is tied to the project budget.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 131
Which of the following is considered one of the most frequent failures in project management?

A. Overly restrictive management
B. Insufficient resources
C. Excessive personnel on project
D. Failure to meet project deadlines

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 132
A recommended method to document the respective roles of groups and individuals for a given process is to:

A. Develop a detailed internal organization chart
B. Develop an isolinear response matrix with cost benefit analysis projections
C. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
D. Develop a telephone call tree for emergency response

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 133
This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

A. Scope creep
B. Deadline extension
C. Deliverable expansion
D. Scope modification

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
QUESTION 134
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 conditional
B. Risk minimal
C. Risk tolerant
D. Risk averse

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 135
The security team has investigated the theft/loss of several unencrypted laptop computers containing sensitive corporate information. To prevent the loss of any additional corporate data it is unilaterally decided by the CISO that all existing and future laptop computers will be encrypted. Soon, the help desk is flooded with complaints about the slow performance of the laptops and users are upset.

What did the CISO do wrong?

A. Failed to identify all stakeholders and their needs
B. Deployed the encryption solution in an inadequate manner
C. Used 1024 bit encryption when 256 bit would have sufficed
D. Used hardware encryption instead of software encryption

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 136
An example of professional unethical behavior is:

A. Sharing copyrighted material with other members of a professional organization where all members have legitimate access to the material
B. Copying documents from an employer’s server which you assert that you have an intellectual property claim to possess, but the company disputes
C. Storing client lists and other sensitive corporate internal documents on a removable thumb drive
D. Gaining access to an affiliated employee’s work email account as part of an officially sanctioned internal investigation

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 137

When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

A. Vendor uses their own laptop and logins using two factor authentication with their own unique credentials
B. Vendor uses a company supplied laptop and logins using two factor authentication wit same admin credentials your security team uses
C. Vendor uses a company supplied laptop and logins using two factor authentication with their own unique credentials
D. Vendors uses their own laptop and logins with same admin credentials your security team uses

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 138

Which of the following is critical in creating a security program aligned with an organization's goals?

A. Develop a culture in which users, managers and IT professionals all make good decisions about information risk
B. Provide clear communication of security program support requirements and audit schedules
C. Create security awareness programs that include clear definition of security program goals and charters
D. Ensure security budgets enable technical acquisition and resource allocation based in internal compliance requirements

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 139

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 sever revenue disruptions.

Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?

A. Audit and Compliance
B. The CFO
C. The CISO

D. The business owner

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 140
A newly appointed security officer finds data leakage software licenses that had never been used. The officer decides to implement a project to ensure it gets installed, but the project gets a great deal of resistance across the organization.

Which of the following represents the MOST likely reason for this situation?

A. The project was initiated without an effort to get support from impacted business units in the organization
B. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects
C. The software is out of date and does not provide for a scalable solution across the enterprise
D. The software license expiration is probably out of synchronization with other software licenses

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
QUESTION 141
The company decides to release the application without remediating the high-risk vulnerabilities.

Which of the following is the MOST likely reason for the company to release the application?

A. The company does not believe the security vulnerabilities to be real
B. The company lacks the tools to perform a vulnerability assessment
C. The company lacks a risk management process
D. The company has a high risk tolerance

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 142
Which of the following best summarizes the primary goal of a security program?

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

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 143
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization.

Which of the following principles does this best demonstrate?
A. Proper budget management B.
Leveraging existing implementations
C. Alignment with the business
D. Effective use of existing technologies

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 144
A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization.

Which of the following principles does this best demonstrate?

A. Proper budget management
B. Leveraging existing implementations

C. Alignment with the business
D. Effective use of existing technologies

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145
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 complete inventory of Information technology assets including infrastructure, networks, applications and data
B. A security organization that is adequately staffed to apply required mitigation strategies and regulatory compliance solutions
C. A clear set of security policies and procedures that are more concept-based than controls-based than controls-based
D. A clearly identified executive sponsor who will champion the effort to ensure organizational buy-in

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
Which of the following is considered a project versus a managed process?

A. ongoing risk assessment of routine operations
B. continuous vulnerability assessment and vulnerability repair
C. monitoring external and internal environment during incident response
D. installation of a new firewall system

Correct Answer: D
Section: (none)

Explanation

Explanation/Reference:

QUESTION 147

A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets.

This demonstrates which of the following principles?

A. Increased security program presence
B. Regulatory compliance effectiveness
C. Security organizational policy enforcement
D. Proper organizational policy enforcement

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 148

Which of the following methodologies references the recommended industry standard that Information security project managers should follow?

A. The Security Systems Development Life Cycle
B. Project Management System Methodology
C. Project Management Body of Knowledge
D. The Security Project and Management Methodology

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 149

Which of the following can the company implement in order to avoid this type of security issue in the future?

A. Network based intrusion detection systems
B. An audit management process

C. A security training program for developers
D. A risk management process

Correct Answer: C **Section:**
(none) Explanation

Explanation/Reference:

QUESTION 150
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do.

What can John do in this instance?
A. Withhold the vendor's payments until the issue is resolved.
B. refer to the contract agreement for direction.
C. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
D. Review the Request for proposal (RFP) for guidance.

Correct Answer: B
Section: (none) Explanation

Explanation/Reference:

QUESTION 151
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. Certificate authority key
B. the recipient's private key
C. The recipient's public key
D. Your public key

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 152

When dealing with risk, the information security practitioner may choose to:

A. acknowledge
B. transfer
C. assign
D. defer

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

A. Single Loss Expectancy
B. Life Cycle Loss Expectancy
C. Safeguard Value
D. Cost Benefit Analysis

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 154

Human resource planning for security professionals in your organization is a:

A. Training requirement that is on-going and always changing.
B. Simple and easy task because the threats are getting easier to find and correct.
C. Training requirement that is met through once every year user training.

D. Not needed because automation and anti-virus software has eliminated the threats.

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 155
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand.

You should:

A. Create a detailed technical executive summary
B. Create timelines for mitigation
C. Calculate annual loss expectancy
D. Develop a cost-benefit analysis

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 156
What is the BEST reason for having a formal request for proposal process?

A. Creates a timeline for purchasing and budgeting
B. Informs suppliers a company is going to make a purchase
C. Clearly identifies risks and benefits before funding is spent
D. Allows small companies to compete with larger companies

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 157
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. Public
B. Administrator
C. Execute
D. Read

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 158
As the CISO you need to write the IT security strategic plan.

Which of the following is the MOST important to review before you start writing the plan?

A. The existing IT environment
B. Other corporate technology trends
C. The company business plan
D. The present IT budget

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 159
The rate of change in technology increases the importance of:

A. Hiring personnel with leading edge skills.
B. Understanding user requirements.

C. Outsourcing the IT functions.
D. Implementing and enforcing good processes.

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:
QUESTION 160
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 patch systems as needed
C. Unable to run anti-virus scans
D. Unable to track log on activity

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 161
When updating the security strategic planning document what two items must be included?

A. Alignment with the business goals and the vision of the CIO
B. The risk tolerance of the company and the company mission statement
C. The alignment with the business goals and the risk tolerance
D. The executive summary and vision of the board of directors

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162
Your incident handling manager detects a virus attack in the network of your company. You develop a signature based on the characteristics of the detected virus.

Which of the following phases in the incident handling process will utilize the signature to resolve this incident?

A. Eradication
B. Containment
C. Recovery
D. Identification

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 163
A system is designed to dynamically block offending Internet IP-addresses from requesting services from a secure website.

This type of control is considered_______________________.

A. Preventive detection control
B. Corrective security control
C. Zero-day attack mitigation
D. Dynamic blocking control

Correct Answer: B **Section: (none) Explanation**

Explanation/Reference:

QUESTION 164
Which of the following is a countermeasure to prevent unauthorized database access from web applications?

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

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 165

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

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

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 166

An anonymity network is a series of?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167

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. Deep-Packet inspection
B. Traffic Analysis
C. Heuristic analysis

D. Packet sampling

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 168
Which wireless encryption technology makes use of temporal keys?

A. Wi-Fi Protected Access version 1 (WPA2)
B. Wireless Equivalence Protocol (WEP)
C. Wireless Application Protocol (WAP)
D. Extensible Authentication Protocol (EAP)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called____________________.

A. Security certification
B. Security accreditation
C. Alignment with business practices and goals.
D. Security system analysis

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
QUESTION 170
The ability to demand the implementation and management of security controls on third parties providing services to an organization is_________________________.

A. Disaster recovery
B. Security Governance
C. Vendor management
D. Compliance management

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 171
Security related breaches are assessed and contained through which of the following?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
What type of attack requires the least amount of technical equipment and has the highest success rate?

A. Social engineering
B. Shrink wrap attacks
C. Operating system attacks
D. War driving
Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 173

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

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 174

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

A. “DROPTABLE USERNAME”
B. NOPS
C. /../../../../
D. ‘O 1=1 - -

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 175

When analyzing and forecasting a capital expense budget what are not included?

A. Purchase of new mobile devices to improve operations
B. New datacenter to operate from
C. Network connectivity costs
D. Upgrade of mainframe

Correct Answer: C
Section: (none) Explanation

Explanation/Reference:

QUESTION 176
Which of the following is MOST useful when developing a business case for security initiatives?

A. Cost/benefit analysis
B. Budget forecasts
C. Vendor management
D. Request for proposals

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 177
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. Privacy protection
C. data security system
D. data classification

Correct Answer: D
Section: (none) Explanation

Explanation/Reference:

QUESTION 178
What is the FIRST step in developing the vulnerability management program?

A. Baseline the Environment

B. Define policy
C. Maintain and Monitor
D. Organization Vulnerability

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 179
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 UDP port 22
D. It uses TCP port 22 as the default port and operates at the application layer

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 180
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements.

During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.

What action should you take FIRST?

A. Consult with other C-Level executives to develop an action plan
B. Contract with a credit reporting company for paid monitoring services for affected customers
C. Contact your local law enforcement agency
D. Destroy the repository of stolen data

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 181
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information.

All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. The organization wants a more permanent solution to the threat to user credential compromise through phishing.

What technical solution would BEST address this issue?

A. Multi-factor authentication employing hard tokens
B. Forcing password changes every 90 days
C. Decreasing the number of employees with administrator privileges
D. Professional user education on phishing conducted by a reputable vendor

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:
QUESTION 182
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country.

Your team now has full access to the data on the foreign server. Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time.

Which technology or solution could you deploy to prevent employees from removing corporate data from your network?

A. Rigorous syslog reviews

B. Intrusion Detection Systems (IDS)
C. Security Guards posted outside the Data Center
D. Data Loss Prevention (DLP)

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.

Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

A. Payment Card Industry Digital Security Standard (PCI DSS)
B. National Institute of Standards and Technology (NIST) Special Publication 800-53
C. International Organization for Standardization – ISO 27001/2
D. British Standard 7799 (BS7799)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
Scenario: Critical servers show signs of erratic behavior within your organization’s intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team. During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions.

What is the MOST critical aspect of the team’s activities?

A. Regular communication of incident status to executives
B. Preservation of information
C. Eradication of malware and system restoration
D. Determination of the attack source

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Scenario: As you begin to develop the program for your organization, you assess the corporate culture and determine that there is a pervasive opinion that the security program only slows things down and limits the performance of the "real workers." Which group of people should be consulted when developing your security program?

A. Peers
B. End Users
C. All of the above
D. Executive Management

Correct Answer: C
Section: (none)
Explanation
Explanation/Reference:

QUESTION 186
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget. Using the best business practices for project management, you determine that the project correctly aligns with the organization goals.

What should be verified next?

A. Scope
B. Constraints
C. Resources

D. Budget

Correct Answer: A
Section: (none) Explanation

Explanation/Reference:

QUESTION 187
Scenario: The new CISO was informed of all the Information Security projects that the section has in progress. Two projects are over a year behind schedule and way over budget.

Which of the following will be most helpful for getting an Information Security project that is behind schedule back on schedule?

A. Upper management support
B. Involve internal audit
C. More frequent project milestone meetings
D. More training of staff members

Correct Answer: A
Section: (none) Explanation

Explanation/Reference: