712-50.203q

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

712-50

EC-Council Certified CISO (CCISO)

Exam A

QUESTION 1
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 2
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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 11
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 12
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 13
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 14
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 15
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 16
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 17
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. Analyze existing controls on systems
D. Create an architecture gap analysis

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

QUESTION 18
If your organization operates under a model of "assumption of breach", you should:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19
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 20
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 21
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 22
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 23
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 processC. Due Care

 D. Due Protection

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
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 26
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 27

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 28
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 29
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 30
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 31
Which of the following intellectual Property components is focused on maintaining brand recognition?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32
Credit card information, medical data, and government records are all examples of:

A. None
B. Communications Information
C. Bodily Information
D. Confidential/Protected Information
E. Territorial Information

D

QUESTION 33
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
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. Quantitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)
C. Qualitative risk assessments map to business objectives
D. Qualitative risk assessments result in a quantitative assessment (high, medium, low, red, yellow, green)

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
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 Mitigation
B. Risk Acceptance
C. Risk Avoidance
D. Risk Transfer

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
What is the definition of Risk in Information Security?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
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. If the risk 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.
C. Amend the standard to permit the deployment.
D. Permit a 90-day window to see if an issue occurs and then amend the standard if there are no issues.

B

QUESTION 38
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)
Explanation

Explanation/Reference:

QUESTION 39
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

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:
Section: (none)
Explanation

Explanation/Reference:
QUESTION 40
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 41
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 42
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

D

QUESTION 43
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)
Explanation

Explanation/Reference:

QUESTION 44
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:
Section: (none)
Explanation

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

Explanation/Reference:

QUESTION 45
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 46
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 47
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

Section: (none)
Explanation

Explanation/Reference:

QUESTION 48
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 49
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 50

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 51
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 52
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 53
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 54
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 55
You work as a project manager for TYU project. You are planning for risk mitigation. You need to quickly identify high-level risks that will need a more in-depth analysis.

Which of the following activities will help you in this?

A. Risk mitigation
B. Estimate activity duration
C. Quantitative analysis
D. Qualitative analysis

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
A global health insurance company is concerned about protecting confidential information.

Which of the following is of MOST concern to this organization?

A. Alignment with International Organization for Standardization (ISO) standards.
B. Alignment with financial reporting regulations for each country where they operate.

C. Compliance to the payment Card Industry (PCI) regulations.
D. Compliance with patient data protection regulations for each country where they operate.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?
A. Improper use of information resources
B. Reduction of budget
C. Decreased security awareness
D. Fines for regulatory non-compliance

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
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 59
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 60
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 61
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 62
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 63
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 64

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 65
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 66
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 67
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 68
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 69
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 70
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 71
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 72
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 73
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 74
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 75
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 76
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 77
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 78
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 79

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 80
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 81
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 82
Creating a secondary authentication process for network access would be an example of?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
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 84

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 85
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 86
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 employees and users

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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 88
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 89
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 90
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 91
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 92
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 93
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 94
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 95
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 96
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 97
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 98
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 99
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 100
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. Technical Control
B. Management Control
C. Operational Control
D. Training Control

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
A system was hardened at the Operating System level and placed into the production environment. Months later an audit was performed and it identified insecure configuration different from the original hardened state.

Which of the following security issues is the MOST likely reason leading to the audit findings?

A. Lack of asset management processes
B. Lack of hardening standards
C. Lack of proper access controls
D. lack of change management processes

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
When is an application security development project complete?

A. When the application turned over to production.

B. After one year
C. When the application reaches the maintenance phase.
D. When the application is retired.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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. Create technology recovery plans
B. Determine the annual loss expectancy (ALE)
C. Build a secondary hot site
D. Create a crisis management plan

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
Which of the following activities must be completed BEFORE you can calculate risk?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105
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: (none)
Explanation

Explanation/Reference:

QUESTION 106
The effectiveness of an audit is measured by?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 107
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108

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 109
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 110
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 111
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 112
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 113
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 114
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 115
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 116
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 117
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 118
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 119

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 120
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 121
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 122
You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do.

What is the BEST approach to handle this situation?

A. Tune the sensors to help reduce false positives so the team can react better
B. Request additional resources to handle the workload
C. Tell the team to do their best and respond to each alert
D. Tell the team to only respond to the critical and high alerts

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 123
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise.

Which tool selection represents the BEST choice to achieve situational awareness?

A. Intrusion Detection System (IDS), firewall, switch, syslog
B. Security Incident Event Management (SIEM), IDS, router, syslog
C. VMware, router, switch, firewall, syslog, vulnerability management system (VMS)
D. SIEM, IDS, firewall, VMSSIEM, IDS, firewall, VMS

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

QUESTION 124
Information Security is often considered an excessive, after-the-fact cost when a project or initiative is completed.

What can be done to ensure that security is addressed cost effectively?

A. Launch an internal awareness campaign
B. Installation of new firewalls and intrusion detection systems
C. Integrate security requirements into project inception
D. User awareness training for all employees

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 125
Which of the following is the BEST indicator of a successful project?

A. it comes in at or below the expenditures planned for in the baseline budget
B. it meets most of the specifications as outlined in the approved project definition
C. it is completed on time or early as compared to the baseline project plan
D. the deliverables are accepted by the key stakeholders

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 126
Which of the following is the MOST important component of any change management process?

A. Outage planning
B. Scheduling
C. Management approval

D. Back-out procedures

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 127
When selecting a security solution with reoccurring maintenance costs after the first year

A. Implement the solution and ask for the increased operating cost budget when it is time
B. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
C. Defer selection until the market improves and cash flow is positive
D. The CISO should cut other essential programs to ensure the new solution's continued use

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 128
What oversight should the information security team have in the change management process for application security?

A. Information security should be aware of any significant application security changes and work with developer to test for vulnerabilities before changes are deployed in production
B. Information security should be aware of all application changes and work with developers before changes and deployed in production
C. Information security should be informed of changes to applications only
D. Development team should tell the information security team about any application security flaws

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

QUESTION 129
An application vulnerability assessment has identified a security flaw in an application. This is a flaw that was previously identified and remediated on a prior release of the application.

Which of the following is MOST likely the reason for this recurring issue?

A. Lack of version/source controls
B. Lack of change management controls
C. Ineffective configuration management controls
D. High turnover in the application development department

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 130
In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 131
When entering into a third party vendor agreement for security services, at what point in the process is it BEST to understand and validate the security posture and compliance level of the vendor?

A. Prior to signing the agreement and before any security services are being performed

B. Once the agreement has been signed and the security vendor states that they will need access to the network
C. Once the vendor is on premise and before they perform security services
D. At the time the security services are being performed and the vendor needs access to the network

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 132
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 133
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 134
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 135
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 136

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 137

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 138

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 139
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 140
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 141
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 142
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 143

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: (none)
Explanation

Explanation/Reference:

QUESTION 144

Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

A. Terms and Conditions
B. Statements of Work
C. Service Level Agreements (SLA)
D. Key Performance Indicators (KPI)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 145

A CISO sees abnormally high volumes of exceptions to security requirements and constant pressure from business units to change security processes.

Which of the following represents the MOST LIKELY cause of this situation?

A. Poor audit support for the security program
B. Poor alignment of the security program to business needs

C. This is normal since business units typically resist security requirements
D. A lack of executive presence within the security program

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 146
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. Incident response
B. Risk assessment
C. Planning
D. System testing

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 147
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. Risk Management
C. Incident Response
D. Network Security administration

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 148

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 149

As the CISO for your company you are accountable for the protection of information resources commensurate with:

A. Risk of exposure
B. Cost and time to replace
C. Insurability tables
D. Customer demand

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 150

The process of identifying and classifying assets is typically included in the_____.

A. Threat analysis process
B. Business Impact Analysis
C. Asset configuration management process

D. Disaster Recovery plan

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 151
File Integrity Monitoring (FIM) is considered a_____.

A. Network based security preventative control
B. Software segmentation control
C. User segmentation control
D. Security detective control

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 152
What are the primary reasons for the development of a business case for a security project?

A. To forecast usage and cost per software licensing
B. To understand the attack vectors and attack sources
C. To communicate risk and forecast resource needs
D. To estimate risk and negate liability to the company

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 153
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 154
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 155
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 156
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 157
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 158
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 159
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 160
The newly appointed CISO of an organization is reviewing the IT security strategic plan.

Which of the following is the MOST important component of the strategic plan?

A. There is a clear definition of the IT security mission and vision.
B. The plan requires return on investment for all security projects.
C. There is integration between IT security and business staffing
D. There is an auditing methodology in place.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 161
Annual Loss Expectancy is derived from the function of which two factors?

A. Annual rate of Occurrence and Single Loss Expectancy
B. Annual rate of Occurrence and Asset Value
C. Safeguard value and Annual Rate of Occurrence
D. Single Loss Expectancy and Exposure factor

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 162

Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of_____.

A. User segmentation controls
B. Software segmentation controls
C. Network based security detective controls
D. Network based security preventative controls

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 163
The formal certification and accreditation process has four primary steps, what are they?

A. Evaluating, describing, testing and authorizing
B. Auditing, documenting, verifying, certifying
C. Evaluating, purchasing, testing, authorizing
D. Discovery, testing, authorizing, certifying

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 164
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. Business continuity plan
B. Application mapping document
C. Disaster recovery strategic plan
D. Enterprise Risk Assessment

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 165
What is the primary reason for performing a return on investment analysis?

A. To determine the current present value of a project
B. To determine the annual rate of loss
C. To decide between multiple vendors
D. To decide is the solution costs less than the risk it is mitigating

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 166
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. Expert forensics witness
B. Fully trained network forensic expects to analyze all data right after the attack
C. Uninterrupted Chain of Custody
D. Comprehensive Log-Files from all servers and network devices affected during the attack

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 167

What is the primary reason for performing vendor management?

A. To define the partnership for long-term success
B. To understand the risk coverage that are being mitigated by the vendor
C. To establish a vendor selection process
D. To document the relationship between the company and vendor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 168
Physical security measures typically include which of the following components?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 169
Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 170
Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

A. The NPV of the project is negative
B. The return on Investment (ROI) is larger than 10 months
C. The Net Present value (NPV) of the project is positive
D. The ROI is lower than 10 months

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 171
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. conflict resolution
B. strong authentication
C. non-repudiation
D. digital rights management

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 172
The process for management approval of the security certification process which states the risks and mitigation of such risks of a given IT system is called_____.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 173
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 are undetectable by software
B. In-line hardware keyloggers are relatively inexpensive
C. In-line hardware keyloggers don't require physical access
D. In-line hardware keyloggers don't comply to industry regulations

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 174
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The cipher text sent by the AP is encrypted with the same key and cipher used by its stations.

What authentication method is being used?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 175
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 176
Which wireless encryption technology makes use of temporal keys?

A. Wi-Fi Protected Access version 2 (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 177
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 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
Which of the following backup sites takes the longest recovery time?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 181
Which of the following is a symmetric encryption algorithm?

A. 3DES
B. RSA
C. ECCD. MD5

Correct Answer: A

Section: (none)
Explanation

Explanation/Reference:

QUESTION 182
When analyzing and forecasting an operating expense budget what are not included?

A. New datacenter to operate from
B. Network connectivity costs
C. Software and hardware license fees
D. Utilities and power costs

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 183
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.

When formulating the remediation plan, what is a required input?

A. Board of directors
B. Latest virus definitions file
C. Patching history
D. Risk assessment

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 184
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.

Your Corporate Information Security Policy should include which of the following?

A. Roles and responsibilities
B. Information security theory
C. Incident response contacts
D. Desktop configuration standards

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 185
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.

What is one proven method to account for common elements found within separate regulations and/or standards?

A. Design your program to meet the strictest government standards
B. Develop a crosswalk
C. Hire a GRC expert
D. Use the Find function of your word processor

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 186

Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations. You have decided to deal with risk to information from people first.

How can you minimize risk to your most sensitive information before granting access?

A. Set your firewall permissions aggressively and monitor logs regularly.
B. Develop an Information Security Awareness program
C. Conduct background checks on individuals before hiring them
D. Monitor employee drowsing and surfing habits

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 187
Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified. The CISO has validated audit findings, determined if compensating controls exist, and started initial remediation planning.

Which of the following is the MOST logical next step?

A. Create detailed remediation funding and staffing plans
B. Report the audit findings and remediation status to business stake holders
C. Validate the effectiveness of current controls
D. Review security procedures to determine if they need modified according to findings

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 188
Scenario: Your program is developed around minimizing risk to information by focusing on people, technology, and operations.

An effective way to evaluate the effectiveness of an information security awareness program for end users, especially senior executives, is to conduct periodic:

A. Baseline of computer systems
B. Password changes
C. Controlled spear phishing campaigns
D. Scanning for viruses

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
QUESTION 189
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.”

What must you do first in order to shift the prevailing opinion and reshape corporate culture to understand the value of information security to the organization?

A. Cite corporate policy and insist on compliance with audit findings
B. Draw from your experience and recount stories of how other companies have been compromised
C. Understand the business and focus your efforts on enabling operations securely
D. Cite compliance with laws, statutes, and regulations – explaining the financial implications for the company for non-compliance

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 190
Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.

Which of the following is the FIRST action the CISO will perform after receiving the audit report?

A. Inform peer executives of the audit results
B. Validate gaps and accepts or dispute the audit findings

C. Create remediation plans to address program gaps
D. Determine if security policies and procedures are adequate

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 191
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 192
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 193
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 194
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget. Using the best business practices for project management you determine that the project correct aligns with the company goals.

What needs to be verified FIRST?

A. Training of the personnel on the project
B. Timeline of the project milestones
C. Vendor for the project
D. Scope of the project

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 195
The new CISO was informed of all the Information Security projects that the organization has in progress. Two projects are over a year behind schedule and over budget. Using best business practices for project management you determine that the project correctly aligns with the company goals.

Which of the following needs to be performed NEXT?

A. Verify technical resources
B. Verify capacity constraints
C. Verify the scope of the project
D. Verify the regulatory requirements

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 196
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.

When multiple regulations or standards apply to your industry you should set controls to meet the_____.

A. Most complex standard
B. Recommendations of your Legal Staff
C. Easiest regulation or standard to implement
D. Stricter regulation or standard

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 197
Scenario: A Chief Information Security Officer (CISO) recently had a third party conduct an audit of the security program. Internal policies and international standards were used as audit baselines. The audit report was presented to the CISO and a variety of high, medium and low rated gaps were identified.

After determining the audit findings are accurate, which of the following is the MOST logical next activity?

A. Validate gaps with the Information Technology team
B. Begin initial gap remediation analyses
C. Review the security organization's charter
D. Create a briefing of the findings for executive management

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 198
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs. You have identified potential solutions for all of your risks that do not have security controls.

What is the NEXT step?

A. Create a risk metrics for all unmitigated risks
B. Get approval from the board of directors
C. Verify that the cost of mitigation is less than the risk
D. Screen potential vendor solutions

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 199
You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget. Using the best business practices for project management you determine that the project correctly aligns with the company goals and the scope of the project is correct.

What is the NEXT step?

A. Verify resources
B. Review time schedules
C. Verify budget
D. Verify constraints

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 200
Scenario: An organization has made a decision to address Information Security formally and consistently by adopting established best practices and industry standards. The organization is a small retail merchant but it is expected to grow to a global customer base of many millions of customers in just a few years.

Which of the following would be the FIRST step when addressing Information Security formally and consistently in this organization?

A. Define formal roles and responsibilities for Information Security
B. Define formal roles and responsibilities for Internal audit functions
C. create an executive security steering committee
D. Contract a third party to perform a security risk assessment

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 201

Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

Symmetric encryption in general is preferable to asymmetric encryption when:

A. The number of unique communication links is large
B. The distance to the end node is farthest away
C. The volume of data being transmitted is small
D. The speed of the encryption / deciphering process is essential

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 202
Scenario: A CISO has several two-factor authentication systems under review and selects the one that is most sufficient and least costly. The implementation project planning is completed and the teams are ready to implement the solution. The CISO then discovers that the product it is not as scalable as originally thought and will not fit the organization's needs. The CISO discovers the scalability issue will only impact a small number of network segments.

What is the next logical step to ensure the proper application of risk management methodology within the two-factor implementation project?

A. Decide to accept the risk on behalf of the impacted business units
B. Create new use cases for operational use of the solution
C. Report the deficiency to the audit team and create process exceptions
D. Determine if sufficient mitigating controls can be applied

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 203
Scenario: Your company has many encrypted telecommunications links for their world-wide operations. Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.

How can you reduce the administrative burden of distributing symmetric keys for your employer?

A. Use certificate authority to distribute private keys
B. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it
C. Use a self-generated key on both ends to eliminate the need for distribution
D. Use asymmetric encryption for the automated distribution of symmetric key

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

https://vceplus.com/