a712-50

Passing Score: 800
Time Limit: 0 min

Exam A

QUESTION 1
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 2
Dataflow diagrams are used by IT auditors to:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
During the course of a risk analysis your IT auditor identified threats and potential impacts. Next, your IT auditor should:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
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. Utilization reports
D. Availability reports

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
IT control objectives are useful to IT auditors as they provide the basis for understanding the:

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

Correct Answer: A

Section: (none)
Explanation
Explanation/Reference:

QUESTION 6

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 7

Which of the following is the MOST important goal of risk management?

A. Identifying the risk
B. Finding economic balance between the impact of the risk and the cost of the control
C. Identifying the victim of any potential exploits.
D. Assessing the impact of potential threats

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 8

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 9
Which of the following activities results in change requests?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 10
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. Single Loss Expectancy (SLE)
B. Exposure Factor (EF)
C. Annualized Rate of Occurrence (ARO)
D. Temporal Probability (TP)

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 11
Which of the following tests is an IS auditor performing when a sample of programs is selected to determine if the source and object versions are the same?

A. A substantive test of program library controls
B. A compliance test of program library controls
C. A compliance test of the program compiler controlsD. A substantive test of the program compiler controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 12
Creating a secondary authentication process for network access would be an example of?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 13
The patching and monitoring of systems on a consistent schedule is required by?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 14
As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 15
As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building. Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?

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

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

QUESTION 16
Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 17
The CIO of an organization has decided to assign the responsibility of internal IT audit to the IT team. This is consider a bad practice MAINLY because

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 18

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 19

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 20

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 21
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 22
A recent audit has identified a few control exceptions and is recommending the implementation of technology and processes to address the finding. Which of the following is the MOST likely reason for the organization to reject the implementation of the recommended technology and processes?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 23
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 24
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 25
The risk found after a control has been fully implemented is called:

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 26
In MOST organizations which group periodically reviews network intrusion detection system logs for all systems as part of their daily tasks?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 27
At which point should the identity access management team be notified of the termination of an employee?

A. At the end of the day once the employee is off site
B. During the monthly review cycle

C. Immediately so the employee account(s) can be disabled
D. Before an audit

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 28
To have accurate and effective information security policies how often should the CISO review the organization policies?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 29
How often should an environment be monitored for cyber threats, risks, and exposures?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 30

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 31

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

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 32

Which represents PROPER separation of duties in the corporate environment?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 33
Creating good security metrics is essential for a CISO. What would be the BEST sources for creating security metrics for baseline defenses coverage?
A. Servers, routers, switches, modem
B. Firewall, exchange, web server, intrusion detection system (IDS)
C. Firewall, anti-virus console, IDS, syslog
D. IDS, syslog, router, switches

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 34
Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture. What would be the BEST choice of security metrics to present to the BOD?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 35
When a critical vulnerability has been discovered on production systems and needs to be fixed immediately, what is the BEST approach for a CISO to mitigate the vulnerability under tight budget constraints?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 36
An information security department is required to remediate system vulnerabilities when they are discovered. Please select the three primary remediation methods that can be used on an affected system.

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 37
When a CISO considers delaying or not remediating system vulnerabilities which of the following are MOST important to take into account?

A. Threat Level, Risk of Compromise, and Consequences of Compromise

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 38
The effectiveness of an audit is measured by?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 39
A new CISO just started with a company and on the CISO's desk is the last complete Information Security Management audit report. The audit report is over two years old. After reading it, what should be the CISO's FIRST priority?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 40

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

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 41

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 42
Which of the following is considered to be an IT governance framework and a supporting toolset that allows for managers to bridge the gap between control requirements, technical issues, and business risks?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
QUESTION 43
Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 44
Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

A. To give information security management recommendations to those who are responsible for initiating, implementing, or maintaining security in theirorganization.
B. To provide a common basis for developing organizational security standards
C. To provide effective security management practice and to provide confidence in inter-organizational dealings

D. To established guidelines and general principles for initiating, implementing, maintaining, and improving information security management within an organization

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 45
Providing oversight of a comprehensive information security program for the entire organization is the primary responsibility of which group under the InfoSec governance framework?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 46
An employee successfully avoids becoming a victim of a sophisticated spear phishing attack due to knowledge gained through the corporate information security awareness program. What type of control has been effectively utilized?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 47
Which of the following illustrates an operational control process:

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 48
With respect to the audit management process, management response serves what function?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 49
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 50
Which of the following are necessary to formulate responses to external audit findings?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 51
The executive board has requested that the CISO of an organization define and Key Performance Indicators (KPI) to measure the effectiveness of the security awareness program provided to call center employees. Which of the following can be used as a KPI?

A. Number of callers who report security issues.
B. Number of callers who report a lack of customer service from the call center
C. Number of successful social engineering attempts on the call center
D. Number of callers who abandon the call before speaking with a representative

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 52
Creating a secondary authentication process for network access would be an example of?

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

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

QUESTION 53
Which of the following activities is the MAIN purpose of the risk assessment process?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 54
Which of the following activities must be completed BEFORE you can calculate risk?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 55
Step-by-step procedures to regain normalcy in the event of a major earthquake is PRIMARILY covered by which of the following plans?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 56
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.

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

Correct Answer: D

Section: (none)
Explanation

Explanation/Reference:

QUESTION 57
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 58
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO) 27001?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 59
The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to

A. assign the responsibility to the information security team.

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 60

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 61

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

A. Meet regulatory compliance requirements

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 62
The mean time to patch, number of virus outbreaks prevented, and number of vulnerabilities mitigated are examples of what type of performance metrics?

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

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

QUESTION 63
When you develop your audit remediation plan what is the MOST important criteria?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 64
Control Objectives for Information and Related Technology (COBIT) is which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 65
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 66
Which of the following represents the BEST reason for an organization to use the Control Objectives for Information and Related Technology (COBIT) as an Information Technology (IT) framework?

A. It allows executives to more effectively monitor IT implementation costs
B. Implementation of it eases an organization’s auditing and compliance burden
C. Information Security (IS) procedures often require augmentation with other standards
D. It provides for a consistent and repeatable staffing model for technology organizations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 67

You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?

A. Validate that security awareness program content includes information about the potential vulnerability
B. Conduct a thorough risk assessment against the current implementation to determine system functions
C. Determine program ownership to implement compensating controls
D. Send a report to executive peers and business unit owners detailing your suspicions

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 68

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 69

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 70
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 change management processes
C. Lack of hardening standards
D. Lack of proper access controls

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 71
Which of the following are not stakeholders of IT security projects?

A. Board of directors
B. Third party vendors
C. CISO
D. Help Desk

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 72
The ultimate goal of an IT security projects is:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 73
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 people on the data center team.
C. Knowing the threats to the organization.
D. Knowing the milestones and timelines of deliverables.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 74
When is an application security development project complete?

A. When the application is retired.
B. When the application turned over to production.
C. When the application reaches the maintenance phase.
D. After one year.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 75
When should IT security project management be outsourced?

A. When organizational resources are limited
B. When the benefits of outsourcing outweigh the inherent risks of outsourcing
C. On new, enterprise-wide security initiatives
D. On projects not forecasted in the yearly budget

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 76
Which business stakeholder is accountable for the integrity of a new information system?

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 77
As the CISO for your company you are accountable for the protection of information resources commensurate with:

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 78
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. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
C. That has budget authority.
D. That will ultimately use the system.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 79

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? (choose the BEST answer):

A. Grant her access, the employee has been adequately warned through the AUP.
B. Assist her with the request, but only after her supervisor signs off on the action.
C. Reset the employee’s password and give it to the supervisor.
D. Deny the request citing national privacy laws.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 80

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? (choose the BEST answer):

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

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 81
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? (choose the BEST answer):

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 82
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 connection/protocol used to transfer the data
C. Type of encryption required for the data once it is at rest
D. Type of computer the data is processed on

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 83
When selecting a security solution with reoccurring maintenance costs after the first year (choose the BEST answer):

A. The CISO should cut other essential programs to ensure the new solution's continued use
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. Implement the solution and ask for the increased operating cost budget when it is time

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 84
Which of the following information may be found in table top exercises for incident response?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
QUESTION 85
Your incident response plan should include which of the following?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 86
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? (choose the best answer):

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 87
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. Extend work hours

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 88
How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) 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 89
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. User awareness training for all employees
B. Installation of new firewalls and intrusion detection systems
C. Launch an internal awareness campaign
D. Integrate security requirements into project inception

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

QUESTION 90
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. Ineffective configuration management controls
B. Lack of change management controls

C. Lack of version/source controls
D. High turnover in the application development department

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 91
Which of the following is the MOST important component of any change management process?

A. Scheduling
B. Back-out procedures
C. Outage planning
D. Management approval

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 92
Which of the following methods are used to define contractual obligations that force a vendor to meet customer expectations?

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 93

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 94

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 95

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

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 96
Which of the following is considered a project versus a managed process?

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

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 97
Which of the following is the BEST indicator of a successful project?
A. it is completed on time or early as compared to the baseline project plan
B. it meets most of the specifications as outlined in the approved project definition
C. it comes in at or below the expenditures planned for in the baseline budget
D. the deliverables are accepted by the key stakeholders

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 98
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. The Security Project And Management Methodology
C. Project Management System Methodology
D. Project Management Body of Knowledge

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 99
This occurs when the quantity or quality of project deliverables is expanded from the original project plan.

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

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

QUESTION 100
Which of the following is considered one of the most frequent failures in project management?

A. Overly restrictive management
B. Excessive personnel on project

C. Failure to meet project deadlines
D. Insufficient resources

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 101
When considering using a vendor to help support your security devices remotely, what is the BEST choice for allowing access?

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 102
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. At the time the security services are being performed and the vendor needs access to the network
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. Prior to signing the agreement and before any security services are being performed

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 103
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 open source security tools and deploy them on your production network
B. Download trial versions of commercially available security tools and deploy on your production network
C. Download open source security tools from a trusted site, test, and then deploy on production network
D. Download security tools from a trusted source and deploy to production network

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 104
The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

A. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
B. Explain to the IT group that the IPS won't cause any network impact because it will fail open
C. Explain to the IT group that this is a business need and the IPS will fail open however, if there is a network failure the CISO will accept responsibility
D. Explain to the IT group that the IPS will fail open once in-line however it will be deployed in monitor mode for a set period of time to ensure that it doesn't block any legitimate traffic

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 105

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

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 106
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. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
B. Intrusion Detection System (IDS), firewall, switch, syslog
C. Security Incident Event Management (SIEM), IDS, router, syslog
D. SIEM, IDS, firewall, VMS

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:
QUESTION 107
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. Tell the team to do their best and respond to each alert
B. Tune the sensors to help reduce false positives so the team can react better
C. Request additional resources to handle the workload
D. Tell the team to only respond to the critical and high alerts

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 108
An example of professional unethical behavior is:

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

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:

QUESTION 109
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's client list of reputable organizations currently using their solution
B. Vendor provided attestation of the detailed security controls from a reputable accounting firm
C. Vendor provided reference from an existing reputable client detailing their implementation
D. Vendor provided internal risk assessment and security control documentation

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:

QUESTION 110

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. Business continuity planning
C. Security Incident Response
D. Thought leadership

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference: