Exam Questions 712-50

EC-Council Certified CISO (CCISO)

https://www.2passeasy.com/dumps/712-50/

NEW QUESTION 1
- (Exam Topic 6)
An auditor is reviewing the security classifications for a group of assets and finds that many of the assets are not correctly classified.
What should the auditor's NEXT step be?

A. Immediately notify the board of directors of the organization as to the finding
B. Correct the classifications immediately based on the auditor's knowledge of the proper classification
C. Document the missing classifications
D. Identify the owner of the asset and induce the owner to apply a proper classification

Answer: C

NEW QUESTION 2
- (Exam Topic 6)
What is the primary difference between regulations and standards?

A. Standards will include regulations
B. Standards that aren't followed are punishable by fines
C. Regulations are made enforceable by the power provided by laws
D. Regulations must be reviewed and approved by the business

Answer: C

NEW QUESTION 3
- (Exam Topic 6)
What is the MOST critical output of the incident response process?

A. A complete document of all involved team members and the support they provided
B. Recovery of all data from affected systems
C. Lessons learned from the incident, so they can be incorporated into the incident response processes
D. Clearly defined documents detailing standard evidence collection and preservation processes

Answer: C

Explanation:
Reference: https://www.eccouncil.org/incident-response-plan-phases/

NEW QUESTION 4
- (Exam Topic 6)
A cloud computing environment that is bound together by technology that allows data and applications to be shared between public and private clouds is BEST referred to as a?

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

Answer: D

Explanation:
Reference:
https://www.datacenters.com/services/cloud-services#:~:text=Hybrid%20clouds%20combine%20public%20and

NEW QUESTION 5
- (Exam Topic 6)
Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye.
However, authorization failures can occur with individuals who have?

A. Glaucoma or cataracts
B. Two different colored eyes (heterochromia iridium)
C. Contact lens
D. Malaria

Answer: A

NEW QUESTION 6
- (Exam Topic 6)
Which of the following strategies provides the BEST response to a ransomware attack?

A. Real-time off-site replication
B. Daily incremental backup
C. Daily full backup
D. Daily differential backup

Answer: B

NEW QUESTION 7
- (Exam Topic 6)
A university recently hired a CISO. One of the first tasks is to develop a continuity of operations plan (COOP). In developing the business impact assessment (BIA), which of the following MOST closely relate to the data
backup and restoral?

A. Recovery Point Objective (RPO)
B. Mean Time to Delivery (MTD)
C. Recovery Time Objective (RTO)
D. Maximum Tolerable Downtime (MTD)

Answer: C

Explanation:
Reference:
https://www.druva.com/glossary/what-is-a-recovery-point-objective-definition-and-related-faqs/#:~:text=The%2

NEW QUESTION 8
- (Exam Topic 6)
A key cybersecurity feature of a Personal Identification Verification (PIV) Card is:

A. Inability to export the private certificate/key
B. It can double as physical identification at the DMV
C. It has the user's photograph to help ID them
D. It can be used as a secure flash drive

Answer: C

Explanation:
Reference: https://www.securew2.com/blog/piv-personal-identity-verification

NEW QUESTION 9
- (Exam Topic 6)
The Board of Directors of a publicly-traded company is concerned about the security implications of a strategic project that will migrate 50% of the organization's information technology assets to the cloud. They have requested a briefing on the project plan and a progress report of the security stream of the project. As the CISO, you have been tasked with preparing the report for the Chief Executive Officer to present.
Using the Earned Value Management (EVM), what does a Cost Variance (CV) of -1,200 mean?

A. The project is over budget
B. The project budget has reserves
C. The project cost is in alignment with the budget
D. The project is under budget

Answer: A

Explanation:
Reference:
https://www.pmi.org/learning/library/earned-value-management-systems-analysis-8026#:~:text=The%20cost%2

NEW QUESTION 10
- (Exam Topic 6)
What does RACI stand for?

A. Reasonable, Actionable, Controlled, and Implemented
B. Responsible, Actors, Consult, and Instigate
C. Responsible, Accountable, Consulted, and Informed
D. Review, Act, Communicate, and Inform

Answer: C

Explanation:
Reference: https://www.google.com/search?q=What+does+RACI+stand+for&oq=What+does+RACI+stand+for&aqs=edge

NEW QUESTION 10
- (Exam Topic 6)
Of the following types of SOCs (Security Operations Centers), which one would be MOST likely used if the CISO has decided to outsource the infrastructure and administration of it?

A. Virtual
B. Dedicated
C. Fusion
D. Command

Answer: A

Explanation:
Reference: https://www.techtarget.com/searchsecurity/definition/Security-Operations-Center-SOC

NEW QUESTION 15
- (Exam Topic 6)
What is a Statement of Objectives (SOA)?

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

Answer: A

NEW QUESTION 18
- (Exam Topic 6)
When reviewing a Solution as a Service (SaaS) provider's security health and posture, which key document should you review?

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

Answer: B

Explanation:
Reference: https://www.threatstack.com/blog/how-saas-companies-can-build-a-compliance-roadmap

NEW QUESTION 21
- (Exam Topic 6)
ABC Limited has recently suffered a security breach with customers' social security number available on the dark web for sale. The CISO, during the time of the incident, has been fired, and you have been hired as the replacement. The analysis of the breach found that the absence of an insider threat program, lack of least privilege policy, and weak access control was to blame. You would like to implement key performance indicators to mitigate the risk.
Which metric would meet the requirement?

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

Answer: C

NEW QUESTION 23
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 27
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 29
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 33
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 36
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 39
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 41
- (Exam Topic 2)
Which of the following is a fundamental component of an audit record?

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

Answer: A

NEW QUESTION 43
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 44
- (Exam Topic 2)
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 controls
D. A substantive test of the program compiler controls

Answer: B

NEW QUESTION 46
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 49
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 50
- (Exam Topic 1)
What is the SECOND step to creating a risk management methodology according to the National Institute of Standards and Technology (NIST) SP 800-30 standard?

A. Determine appetite
B. Evaluate risk avoidance criteria
C. Perform a risk assessment
D. Mitigate risk

Answer: D

NEW QUESTION 54
- (Exam Topic 1)
Which of the following is used to establish and maintain a framework to provide assurance that information security strategies are aligned with organizational objectives?

A. Awareness
B. Compliance
C. Governance
D. Management

Answer: C

NEW QUESTION 57
- (Exam Topic 1)
What should an organization do to ensure that they have a sound Business Continuity (BC) Plan?

A. Test every three years to ensure that things work as planned
B. Conduct periodic tabletop exercises to refine the BC plan
C. Outsource the creation and execution of the BC plan to a third party vendor
D. Conduct a Disaster Recovery (DR) exercise every year to test the plan

Answer: B

NEW QUESTION 58
- (Exam Topic 1)
When choosing a risk mitigation method what is the MOST important factor?

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

Answer: B

NEW QUESTION 60
- (Exam Topic 1)
What two methods are used to assess risk impact?

A. Cost and annual rate of expectance
B. Subjective and Objective
C. Qualitative and percent of loss realized
D. Quantitative and qualitative

Answer: D

NEW QUESTION 65
- (Exam Topic 1)
Which of the following is the MOST important benefit of an effective security governance process?

A. Reduction of liability and overall risk to the organization
B. Better vendor management
C. Reduction of security breaches
D. Senior management participation in the incident response process

Answer: A

NEW QUESTION 70
- (Exam Topic 1)
Risk appetite directly affects what part of a vulnerability management program?

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

Answer: B

NEW QUESTION 73
- (Exam Topic 1)
A business unit within your organization intends to deploy a new technology in a manner that places it in violation of existing information security standards. What immediate action should the information security manager take?

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

Answer: C

NEW QUESTION 77
- (Exam Topic 1)
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, mitigation response time, and cost
B. Attack vectors, controls cost, and investigation staffing needs
C. Vulnerability exploitation, attack recovery, and mean time to repair
D. Susceptibility to attack, expected duration of attack, and mitigation availability

Answer: A

NEW QUESTION 81
- (Exam Topic 1)
After a risk assessment is performed, a particular risk is considered to have the potential of costing the organization 1.2 Million USD. This is an example of

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

Answer: D

NEW QUESTION 83
- (Exam Topic 1)
A method to transfer risk is to:

A. Implement redundancy
B. move operations to another region
C. purchase breach insurance
D. Alignment with business operations

Answer: C

NEW QUESTION 86
- (Exam Topic 1)
Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

A. Reduction of budget
B. Decreased security awareness
C. Improper use of information resources
D. Fines for regulatory non-compliance

Answer: D

NEW QUESTION 88
- (Exam Topic 1)
A company wants to fill a Chief Information Security Officer position in the organization. They need to define
and implement a more holistic security program. Which of the following qualifications and experience would be MOST desirable to find in a candidate?

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

Answer: B

NEW QUESTION 91
- (Exam Topic 1)
Which of the following is the MOST important for a CISO to understand when identifying threats?

A. How vulnerabilities can potentially be exploited in systems that impact the organization
B. How the security operations team will behave to reported incidents
C. How the firewall and other security devices are configured to prevent attacks
D. How the incident management team prepares to handle an attack

Answer: A

NEW QUESTION 94
- (Exam Topic 1)
Which of the following is the MAIN reason to follow a formal risk management process in an organization that hosts and uses privately identifiable information (PII) as part of their business models and processes?

A. Need to comply with breach disclosure laws
B. Need to transfer the risk associated with hosting PII data
C. Need to better understand the risk associated with using PII data
D. Fiduciary responsibility to safeguard credit card information

Answer: C

NEW QUESTION 97
- (Exam Topic 1)
The PRIMARY objective of security awareness is to:

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

Answer: B

NEW QUESTION 100
- (Exam Topic 1)
When would it be more desirable to develop a set of decentralized security policies and procedures within an enterprise environment?

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

Answer: B

NEW QUESTION 105
- (Exam Topic 1)
Who is responsible for securing networks during a security incident?

A. Chief Information Security Officer (CISO)
B. Security Operations Center (SO
C. Disaster Recovery (DR) manager
D. Incident Response Team (IRT)

Answer: D

NEW QUESTION 106
- (Exam Topic 1)
Which of the following is MOST likely to be discretionary?

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

Answer: C

NEW QUESTION 109

- (Exam Topic 1)
You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

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

Answer: C

NEW QUESTION 112
- (Exam Topic 1)
Which of the following intellectual Property components is focused on maintaining brand recognition?

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

Answer: A

NEW QUESTION 116
- (Exam Topic 1)
Risk that remains after risk mitigation is known as

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

Answer: B

NEW QUESTION 118
- (Exam Topic 1)
You have implemented a new security control. Which of the following risk strategy options have you engaged in?

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

Answer: D

NEW QUESTION 122
- (Exam Topic 1)
Risk is defined as:

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

Answer: A

NEW QUESTION 124
- (Exam Topic 1)
The single most important consideration to make when developing your security program, policies, and processes is:

A. Budgeting for unforeseen data compromises
B. Streamlining for efficiency
C. Alignment with the business
D. Establishing your authority as the Security Executive

Answer: C

NEW QUESTION 126
- (Exam Topic 1)
Which of the following is a critical operational component of an Incident Response Program (IRP)?

A. Weekly program budget reviews to ensure the percentage of program funding remains constant.
B. Annual review of program charters, policies, procedures and organizational agreements.
C. Daily monitoring of vulnerability advisories relating to your organization’s deployed technologies.
D. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization

Answer: C

NEW QUESTION 131
- (Exam Topic 1)
The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

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

Answer: B

NEW QUESTION 132
- (Exam Topic 1)
The exposure factor of a threat to your organization is defined by?

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

Answer: D

NEW QUESTION 136
- (Exam Topic 1)
A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?

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

Answer: A

NEW QUESTION 137
- (Exam Topic 1)
The establishment of a formal risk management framework and system authorization program is essential. The LAST step of the system authorization process is:

A. Contacting the Internet Service Provider for an IP scope
B. Getting authority to operate the system from executive management
C. Changing the default passwords
D. Conducting a final scan of the live system and mitigating all high and medium level vulnerabilities

Answer: B

NEW QUESTION 141
- (Exam Topic 1)
What is the MAIN reason for conflicts between Information Technology and Information Security programs?

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

Answer: D

NEW QUESTION 142
- (Exam Topic 1)
When briefing senior management on the creation of a governance process, the MOST important aspect should be:

A. information security metrics.
B. knowledge required to analyze each issue.
C. baseline against which metrics are evaluated.
D. linkage to business area objectives.

Answer: D

NEW QUESTION 147
- (Exam Topic 1)
Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer:

A

NEW QUESTION 149
- (Exam Topic 1)
Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

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

Answer: D

NEW QUESTION 154
- (Exam Topic 1)
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. Scan a representative sample of systems
B. Perform the scans only during off-business hours
C. Decrease the vulnerabilities within the scan tool settings
D. Filter the scan output so only pertinent data is analyzed

Answer: A

NEW QUESTION 157
- (Exam Topic 1)
Which of the following should be determined while defining risk management strategies?

A. Organizational objectives and risk tolerance
B. Risk assessment criteria
C. IT architecture complexity
D. Enterprise disaster recovery plans

Answer: A

NEW QUESTION 162
- (Exam Topic 1)
Who in the organization determines access to information?

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

Answer: C

NEW QUESTION 167
- (Exam Topic 6)
What are the common data hiding techniques used by criminals?

A. Unallocated space and masking
B. Website defacement and log manipulation
C. Disabled Logging and admin elevation
D. Encryption, Steganography, and Changing Metadata/Timestamps

Answer: D

Explanation:
Reference: https://cisomag.eccouncil.org/challenges-and-applications-of-digital-forensics/

NEW QUESTION 170
- (Exam Topic 6)
You have been promoted to the CISO of a big-box retail store chain reporting to the Chief Information Officer (CIO). The CIO's first mandate to you is to develop a cybersecurity compliance framework that will meet all the store's compliance requirements.
Which of the following compliance standard is the MOST important to the organization?

A. The Federal Risk and Authorization Management Program (FedRAMP)
B. ISO 27002
C. NIST Cybersecurity Framework
D. Payment Card Industry (PCI) Data Security Standard (DSS)

Answer: D

Explanation:
Reference:

https://searchcompliance.techtarget.com/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard

NEW QUESTION 172
- (Exam Topic 6)
To make sure that the actions of all employees, applications, and systems follow the organization's rules and regulations can BEST be described as which of the following?

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

Answer: D

Explanation:
Reference: https://www.eccouncil.org/information-security-management/

NEW QUESTION 175
- (Exam Topic 6)
Who should be involved in the development of an internal campaign to address email phishing?

A. Business unit leaders, CIO, CEO
B. Business Unite Leaders, CISO, CIO and CEO
C. All employees
D. CFO, CEO, CIO

Answer: B

NEW QUESTION 176
- (Exam Topic 6)
When evaluating a Managed Security Services Provider (MSSP), which service(s) is/are most important:

A. Patch management
B. Network monitoring
C. Ability to provide security services tailored to the business' needs
D. 24/7 tollfree number

Answer: C

Explanation:
Reference: https://digitalguardian.com/blog/how-hire-evaluate-managed-security-service-providers-mssps

NEW QUESTION 179
- (Exam Topic 6)
What is a key policy that should be part of the information security plan?

A. Account management policy
B. Training policy
C. Acceptable Use policy
D. Remote Access policy

Answer: C

Explanation:
Reference: https://www.exabeam.com/information-security/information-security-policy/

NEW QUESTION 184
- (Exam Topic 6)
A CISO must conduct risk assessments using a method where the Chief Financial Officer (CFO) receives impact data in financial terms to use as input to select the proper level of coverage in a new cybersecurity insurance policy.
What is the MOST effective method of risk analysis to provide the CFO with the information required?

A. Conduct a quantitative risk assessment
B. Conduct a hybrid risk assessment
C. Conduct a subjective risk assessment
D. Conduct a qualitative risk assessment

Answer: D

NEW QUESTION 187
- (Exam Topic 5)
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 compliance with laws, statutes, and regulations – explaining the financial implications for the company for non-compliance

B. Understand the business and focus your efforts on enabling operations securely
C. Draw from your experience and recount stories of how other companies have been compromised
D. Cite corporate policy and insist on compliance with audit findings

Answer: B

NEW QUESTION 190
- (Exam Topic 6)
As the Risk Manager of an organization, you are task with managing vendor risk assessments. During the assessment, you identified that the vendor is engaged with high profiled clients, and bad publicity can jeopardize your own brand.
Which is the BEST type of risk that defines this event?

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

Answer: B

NEW QUESTION 191
- (Exam Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.
Recently, members of your organization have been targeted through a number of sophisticated phishing attempts and have compromised their system credentials.
What action can you take to prevent the misuse of compromised credentials to change bank account information from outside your organization while still allowing employees to manage their bank information?

A. Turn off VPN access for users originating from outside the country
B. Enable monitoring on the VPN for suspicious activity
C. Force a change of all passwords
D. Block access to the Employee-Self Service application via VPN

Answer: D

NEW QUESTION 195
- (Exam Topic 5)
Which of the following best describes the sensors designed to project and detect a light beam across an area?

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

Answer: D

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

NEW QUESTION 199
- (Exam Topic 5)
Using the Transport Layer Security (TLS) protocol enables a client in a network to be:

A. Provided with a digital signature
B. Assured of the server's identity
C. Identified by a network
D. Registered by the server

Answer: B

Explanation:
Reference: https://ukdiss.com/examples/tls.php

NEW QUESTION 202
- (Exam Topic 5)
Which of the following is true regarding expenditures?

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

Answer: D

NEW QUESTION 203

- (Exam Topic 5)
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 adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?

A. Annually
B. Semi-annually
C. Quarterly
D. Never

Answer: D

NEW QUESTION 204
- (Exam Topic 5)
What are the three stages of an identity and access management system?

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

Answer: A

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

NEW QUESTION 205
- (Exam Topic 5)
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. Contract a third party to perform a security risk assessment
B. Define formal roles and responsibilities for Internal audit functions
C. Define formal roles and responsibilities for Information Security
D. Create an executive security steering committee

Answer: C

NEW QUESTION 209
- (Exam Topic 5)
A CISO wants to change the defense strategy to ward off attackers. To accomplish this the CISO is looking to a strategy where attackers are lured into a zone of a safe network where attackers can be monitored, controlled, quarantined, or eradicated.

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

Answer: D

NEW QUESTION 210
- (Exam Topic 5)
An organization has a number of Local Area Networks (LANs) linked to form a single Wide Area Network (WAN). Which of the following would BEST ensure network continuity?

A. Third-party emergency repair contract
B. Pre-built servers and routers
C. Permanent alternative routing
D. Full off-site backup of every server

Answer: C

NEW QUESTION 214
- (Exam Topic 5)
Access Control lists (ACLs), Firewalls, and Intrusion Prevention Systems are examples of

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

Answer: A

NEW QUESTION 218
- (Exam Topic 5)
Scenario: You are the newly hired Chief Information Security Officer for a company that has not previously had a senior level security practitioner. The company

lacks a defined security policy and framework for their Information Security Program. Your new boss, the Chief Financial Officer, has asked you to draft an outline of a security policy and recommend an industry/sector neutral information security control framework for implementation.
Which of the following industry / sector neutral information security control frameworks should you recommend for implementation?

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

Answer: C

NEW QUESTION 221
- (Exam Topic 5)
The ability to demand the implementation and management of security controls on third parties providing services to an organization is

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

Answer: C

NEW QUESTION 223
- (Exam Topic 5)
As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?

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

Answer: A

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

NEW QUESTION 225
- (Exam Topic 5)
Human resource planning for security professionals in your organization is a:

A. Simple and easy task because the threats are getting easier to find and correct.
B. Training requirement that is met through once every year user training.
C. Training requirement that is on-going and always changing.
D. Not needed because automation and anti-virus software has eliminated the threats.

Answer: C

NEW QUESTION 229
- (Exam Topic 5)
During the last decade, what trend has caused the MOST serious issues in relation to physical security?

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

Answer: A

NEW QUESTION 231
- (Exam Topic 5)
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 implemented remediation activities. Which of the following is the MOST logical next step?

A. Validate the effectiveness of applied controls
B. Validate security program resource requirements
C. Report the audit findings and remediation status to business stake holders
D. Review security procedures to determine if they need modified according to findings

Answer: A

NEW QUESTION 233
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.

From an Information Security Leadership perspective, which of the following is a MAJOR concern about the CISO's approach to security?

A. Lack of risk management process
B. Lack of sponsorship from executive management
C. IT security centric agenda
D. Compliance centric agenda

Answer: C

NEW QUESTION 235
- (Exam Topic 5)
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 frameworks and standards will BEST fit the organization as a baseline for their security program?

A. NIST and Privacy Regulations
B. ISO 27000 and Payment Card Industry Data Security Standards
C. NIST and data breach notification laws
D. ISO 27000 and Human resources best practices

Answer: B

NEW QUESTION 240
- (Exam Topic 5)
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. Validate the effectiveness of current controls
B. Create detailed remediation funding and staffing plans
C. Report the audit findings and remediation status to business stake holders
D. Review security procedures to determine if they need modified according to findings

Answer: C

NEW QUESTION 241
- (Exam Topic 5)
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. Budget
C. Resources
D. Constraints

Answer: A

NEW QUESTION 242
- (Exam Topic 5)
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. Security accreditation
D. Alignment with business practices and goals.

Answer: C

NEW QUESTION 245
- (Exam Topic 5)
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. Begin initial gap remediation analyses
B. Review the security organization's charter
C. Validate gaps with the Information Technology team
D. Create a briefing of the findings for executive management

Answer: A

NEW QUESTION 246
- (Exam Topic 5)
The primary purpose of a risk register is to:

A. Maintain a log of discovered risks
B. Track individual risk assessments
C. Develop plans for mitigating identified risks
D. Coordinate the timing of scheduled risk assessments

Answer: A

Explanation:
Reference: https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/

NEW QUESTION 249
- (Exam Topic 5)
During the 3rd quarter of a budget cycle, the CISO noticed she spent more than was originally planned in her annual budget. What is the condition of her current budgetary posture?

A. The budget is in a temporary state of imbalance
B. The budget is operating at a deficit
C. She can realign the budget through moderate capital expense (CAPEX) allocation
D. She has a surplus of operational expenses (OPEX)

Answer: A

NEW QUESTION 250
- (Exam Topic 5)
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 is unsure of the information provided and orders a vendor proof of concept to validate the system's scalability. This demonstrates which of the following?

A. An approach that allows for minimum budget impact if the solution is unsuitable
B. A methodology-based approach to ensure authentication mechanism functions
C. An approach providing minimum time impact to the implementation schedules
D. A risk-based approach to determine if the solution is suitable for investment

Answer: D

NEW QUESTION 255
- (Exam Topic 5)
Which of the following is a primary method of applying consistent configurations to IT systems?

A. Audits
B. Administration
C. Patching
D. Templates

Answer: C

NEW QUESTION 259
- (Exam Topic 5)
A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

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

Answer: D

NEW QUESTION 264
- (Exam Topic 5)
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.
What is the MOST logical course of action the CISO should take?

A. Review the original solution set to determine if another system would fit the organization's risk appetite and budgetregulatory compliance requirements
B. Continue with the implementation and submit change requests to the vendor in order to ensure required functionality will be provided when needed
C. Continue with the project until the scalability issue is validated by others, such as an auditor or third party assessor
D. Cancel the project if the business need was based on internal requirements versus regulatory compliance requirements

Answer: A

NEW QUESTION 266
- (Exam Topic 5)
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. The organization has already been subject to a significant amount of credit card fraud. Which of the following is the MOST likely reason for this fraud?

A. Lack of compliance to the Payment Card Industry (PCI) standards
B. Ineffective security awareness program
C. Security practices not in alignment with ISO 27000 frameworks
D. Lack of technical controls when dealing with credit card data

Answer: A

NEW QUESTION 267
- (Exam Topic 5)
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 asymmetric encryption for the automated distribution of the symmetric key
B. Use a self-generated key on both ends to eliminate the need for distribution
C. Use certificate authority to distribute private keys
D. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it

Answer: A

NEW QUESTION 270
- (Exam Topic 5)
At what level of governance are individual projects monitored and managed?

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

Answer: D

NEW QUESTION 273
- (Exam Topic 5)
Your company has limited resources to spend on security initiatives. The Chief Financial Officer asks you to prioritize the protection of information resources based on their value to the company. It is essential that you be able to communicate in language that your fellow executives will understand. You should:

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

Answer: B

NEW QUESTION 275
- (Exam Topic 5)
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 executive summary and vision of the board of directors
D. The alignment with the business goals and the risk tolerance

Answer: D

NEW QUESTION 279
- (Exam Topic 5)
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. Effective use of existing technologies
B. Create a comprehensive security awareness program and provide success metrics to business units
C. Proper budget management
D. Leveraging existing implementations

Answer: B

NEW QUESTION 282
- (Exam Topic 5)
When project costs continually increase throughout implementation due to large or rapid changes in customer or user requirements, this is commonly known as:

A. Cost/benefit adjustments
B. Scope creep
C. Prototype issues

D. Expectations management

Answer: B

Explanation:
Reference:
http://www.umsl.edu/~sauterv/analysis/6840_f03_papers/gurlen/

NEW QUESTION 287
- (Exam Topic 5)
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 Net Present Value (NPV) of the project is positive
B. The NPV of the project is negative
C. The Return on Investment (ROI) is larger than 10 months
D. The ROI is lower than 10 months

Answer: B

NEW QUESTION 288
- (Exam Topic 5)
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?

A. Lack of identification of technology stake holders
B. Lack of business continuity process
C. Lack of influence with leaders outside IT
D. Lack of a security awareness program

Answer: C

NEW QUESTION 289
- (Exam Topic 5)
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. Controlled spear phishing campaigns
B. Password changes
C. Baselining of computer systems
D. Scanning for viruses

Answer: A

NEW QUESTION 290
- (Exam Topic 5)
What is the BEST reason for having a formal request for proposal process?

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

Answer: C

NEW QUESTION 291
- (Exam Topic 5)
What is the primary reason for performing vendor management?

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

Answer: A

NEW QUESTION 296
- (Exam Topic 5)
Which of the following is an accurate description of a balance sheet?

A. The percentage of earnings that are retained by the organization for reinvestment in the business
B. The details of expenses and revenue over a long period of time
C. A summarized statement of all assets and liabilities at a specific point in time
D. A review of regulations and requirements impacting the business from a financial perspective

Answer: C

NEW QUESTION 299
- (Exam Topic 5)
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. Conduct background checks on individuals before hiring them
B. Develop an Information Security Awareness program
C. Monitor employee browsing and surfing habits
D. Set your firewall permissions aggressively and monitor logs regularly.

Answer: A

NEW QUESTION 304
- (Exam Topic 5)
The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

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

Answer: B

NEW QUESTION 307
- (Exam Topic 5)
Which of the following best describes revenue?

A. Non-operating financial liabilities minus expenses
B. The true profit-making potential of an organization
C. The sum value of all assets and cash flow into the business
D. The economic benefit derived by operating a business

Answer: D

Explanation:
Reference: https://www.investopedia.com/terms/r/revenue.asp

NEW QUESTION 308
- (Exam Topic 5)
Which type of physical security control scan a person’s external features through a digital video camera before granting access to a restricted area?

A. Iris scan
B. Retinal scan
C. Facial recognition scan
D. Signature kinetics scan

Answer: C

NEW QUESTION 309
- (Exam Topic 5)
Which of the following terms is used to describe countermeasures implemented to minimize risks to physical property, information, and computing systems?

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

Answer: D

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

NEW QUESTION 310
- (Exam Topic 5)
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. Get approval from the board of directors
B. Screen potential vendor solutions
C. Verify that the cost of mitigation is less than the risk
D. Create a risk metrics for all unmitigated risks

Answer: C

NEW QUESTION 312
- (Exam Topic 5)
As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

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

Answer: D

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

NEW QUESTION 315
- (Exam Topic 5)
Smith, the project manager for a larger multi-location firm, is leading a software project team that has 18
members, 5 of which are assigned to testing. Due to recent recommendations by an organizational quality audit team, the project manager is convinced to add a quality professional to lead to test team at additional cost to the project.
The project manager is aware of the importance of communication for the success of the project and takes the step of introducing additional communication channels, making it more complex, in order to assure quality levels of the project. What will be the first project management document that Smith should change in order to accommodate additional communication channels?

A. WBS document
B. Scope statement
C. Change control document
D. Risk management plan

Answer: A

NEW QUESTION 320
- (Exam Topic 5)
What is the difference between encryption and tokenization?

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

Answer: B

Explanation:
Reference:
http://library.ahima.org/doc?oid=104090#.X_dwWolR3eQ

NEW QUESTION 321
- (Exam Topic 5)
Which of the following is the MOST logical method of deploying security controls within an organization?

A. Obtain funding for all desired controls and then create project plans for implementation
B. Apply the simpler controls as quickly as possible and use a risk-based approach for the more difficult andcostly controls
C. Apply the least costly controls to demonstrate positive program activity
D. Obtain business unit buy-in through close communication and coordination

Answer: B

NEW QUESTION 322
- (Exam Topic 5)
Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.
To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

A. Business Impact Analysis
B. Business Continuity plan
C. Security roadmap
D. Annual report to shareholders

Answer: A

NEW QUESTION 327
- (Exam Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN.

Once supervisors and data owners have approved requests, information system administrators will implement

A. Technical control(s)
B. Management control(s)
C. Policy control(s)
D. Operational control(s)

Answer: A

NEW QUESTION 330
- (Exam Topic 5)
A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?

A. Service
B. Program
C. Portfolio
D. Cost center

Answer: B

NEW QUESTION 334
- (Exam Topic 5)
Which of the following is considered the foundation for the Enterprise Information Security Architecture (EISA)?

A. Security regulations
B. Asset classification
C. Information security policy
D. Data classification

Answer: C

NEW QUESTION 338
- (Exam Topic 5)
Which type of scan is used on the eye to measure the layer of blood vessels?

A. Facial recognition scan
B. Iris scan
C. Signature kinetics scan
D. Retinal scan

Answer: D

NEW QUESTION 341
- (Exam Topic 5)
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 system analysis
C. Security accreditation
D. Alignment with business practices and goals.

Answer: A

NEW QUESTION 343
- (Exam Topic 5)
Which of the following is the MOST effective method for discovering common technical vulnerabilities within the IT environment?

A. Reviewing system administrator logs
B. Auditing configuration templates
C. Checking vendor product releases
D. Performing system scans

Answer: D

NEW QUESTION 348
- (Exam Topic 5)
Which of the following would negatively impact a log analysis of a multinational organization?

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

Answer: D

NEW QUESTION 349
- (Exam Topic 5)
Scenario: Your organization employs single sign-on (user name and password only) as a convenience to your employees to access organizational systems and data. Permission to individual systems and databases is vetted and approved through supervisors and data owners to ensure that only approved personnel can use particular applications or retrieve information. All employees have access to their own human resource information, including the ability to change their bank routing and account information and other personal details through the Employee Self-Service application. All employees have access to the organizational VPN. The organization wants a more permanent solution to the threat to user credential compromise through phishing. What technical solution would BEST address this issue?

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

Answer: B

NEW QUESTION 353
- (Exam Topic 5)
As the Chief Information Security Officer, you are performing an assessment of security posture to understand what your Defense-in-Depth capabilities are. Which network security technology examines network traffic flows to detect and actively stop vulnerability exploits and attacks?

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

Answer: B

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

NEW QUESTION 358
- (Exam Topic 4)
The process of identifying and classifying assets is typically included in the

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

Answer: B

NEW QUESTION 360
- (Exam Topic 4)
Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?

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

Answer: A

NEW QUESTION 365
- (Exam Topic 4)
What type of attack requires the least amount of technical equipment and has the highest success rate?

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

Answer: C

NEW QUESTION 369
- (Exam Topic 4)
The ability to hold intruders accountable in a court of law is important. Which of the following activities are needed to ensure the highest possibility for successful prosecution?

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

Answer: A

NEW QUESTION 370

- (Exam Topic 4)
The process for identifying, collecting, and producing digital information in support of legal proceedings is called

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

Answer: B

NEW QUESTION 372
- (Exam Topic 4)
An access point (AP) is discovered using Wireless Equivalent Protocol (WEP). The ciphertext sent by the AP is encrypted with the same key and cipher used by its stations. What authentication method is being used?

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

Answer: A

NEW QUESTION 377
- (Exam Topic 4)
Security related breaches are assessed and contained through which of the following?

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

Answer: C

NEW QUESTION 381
- (Exam Topic 4)
While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

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

Answer: B

NEW QUESTION 383
- (Exam Topic 4)
SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

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

Answer: A

NEW QUESTION 384
- (Exam Topic 4)
As a CISO you need to understand the steps that are used to perform an attack against a network. Put each step into the correct order.
* 1.Covering tracks
* 2.Scanning and enumeration
* 3.Maintaining Access
* 4.Reconnaissance
* 5. Gaining Access

A. 4, 2, 5, 3, 1
B. 2, 5, 3, 1, 4
C. 4, 5, 2, 3, 1
D. 4, 3, 5, 2, 1

Answer: A

NEW QUESTION 386
- (Exam Topic 4)
Network Forensics is the prerequisite for any successful legal action after attacks on your Enterprise Network. Which is the single most important factor to introducing digital evidence into a court of law?

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

Answer: C

NEW QUESTION 389
- (Exam Topic 4)
Which wireless encryption technology makes use of temporal keys?

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

Answer: B

NEW QUESTION 394
- (Exam Topic 4)
What is the term describing the act of inspecting all real-time Internet traffic (i.e., packets) traversing a major Internet backbone without introducing any apparent latency?

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

Answer: B

NEW QUESTION 399
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 404
- (Exam Topic 4)
Which of the following statements about Encapsulating Security Payload (ESP) is true?

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

Answer: A

NEW QUESTION 408
- (Exam Topic 4)
What is the FIRST step in developing the vulnerability management program?

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

Answer: A

NEW QUESTION 412
- (Exam Topic 4)
You are having a penetration test done on your company network and the leader of the team says they discovered all the network devices because no one had changed the Simple Network Management Protocol (SNMP) community strings from the defaults. Which of the following is a default community string?

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

Answer: D

NEW QUESTION 417

- (Exam Topic 3)
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. The CISO
B. Audit and Compliance
C. The CFO
D. The business owner

Answer: D

NEW QUESTION 419
- (Exam Topic 3)
Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?

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

Answer: A

NEW QUESTION 424
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 425
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 426
- (Exam Topic 3)
Which of the following best summarizes the primary goal of a security program?

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

Answer: C

NEW QUESTION 427
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 431
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 435
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 438
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 441
- (Exam Topic 3)
In effort to save your company money which of the following methods of training results in the lowest cost for the organization?

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

Answer: D

NEW QUESTION 442
- (Exam Topic 3)
Which of the following represents the BEST method for obtaining business unit acceptance of security controls within an organization?

A. Allow the business units to decide which controls apply to their systems, such as the encryption of sensitive data
B. Create separate controls for the business units based on the types of business and functions they perform
C. Ensure business units are involved in the creation of controls and defining conditions under which they must be applied
D. Provide the business units with control mandates and schedules of audits for compliance validation

Answer: C

NEW QUESTION 446
- (Exam Topic 3)
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.

Answer: B

NEW QUESTION 449
- (Exam Topic 3)
A recommended method to document the respective roles of groups and individuals for a given process is to:

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

Answer: D

NEW QUESTION 454
- (Exam Topic 3)
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 software license expiration is probably out of synchronization with other software licenses
B. The project was initiated without an effort to get support from impacted business units in the organization
C. The software is out of date and does not provide for a scalable solution across the enterprise
D. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects

Answer: B

NEW QUESTION 458
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 461
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 465
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 467
- (Exam Topic 3)
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.

Answer: A

NEW QUESTION 469
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 472
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 476
- (Exam Topic 3)
Which of the following are not stakeholders of IT security projects?

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

Answer: B

NEW QUESTION 481
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 483
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 485
- (Exam Topic 3)
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. A lack of executive presence within the security program
C. Poor alignment of the security program to business needs
D. This is normal since business units typically resist security requirements

Answer: C

NEW QUESTION 489
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 492
- (Exam Topic 3)
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)

Answer: B

NEW QUESTION 493
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 494
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 499
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 504
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 509
- (Exam Topic 3)
A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

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

Answer: D

NEW QUESTION 510
- (Exam Topic 3)
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

Answer: C

NEW QUESTION 515
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 520
- (Exam Topic 2)
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.

Answer: D

NEW QUESTION 521
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 524
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 527
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 528
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 529
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 534
- (Exam Topic 2)
The implementation of anti-malware and anti-phishing controls on centralized email servers is an example of what type of security control?

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

Answer:

D

NEW QUESTION 537
- (Exam Topic 2)
The regular review of a firewall ruleset is considered a

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

Answer: A

NEW QUESTION 540
- (Exam Topic 2)
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. Procedural control
B. Management control
C. Technical control
D. Administrative control

Answer: B

NEW QUESTION 545
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 546
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 550
- (Exam Topic 2)
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)

Answer: B

NEW QUESTION 552
- (Exam Topic 2)
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)

Answer: A

NEW QUESTION 556
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 557
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 559
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 563
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 566
- (Exam Topic 2)
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

Answer: A

NEW QUESTION 568
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 569
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 570

- (Exam Topic 2)
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

Answer: D

NEW QUESTION 575
- (Exam Topic 2)
Your IT auditor is reviewing significant events from the previous year and has identified some procedural oversights. Which of the following would be the MOST concerning?

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

Answer: A

NEW QUESTION 579
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 583
- (Exam Topic 2)
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)

Answer: C

NEW QUESTION 584
.....

THANKS FOR TRYING THE DEMO OF OUR PRODUCT

Visit Our Site to Purchase the Full Set of Actual 712-50 Exam Questions With Answers.

We Also Provide Practice Exam Software That Simulates Real Exam Environment And Has Many Self-Assessment Features. Order the 712-50 Product From:

https://www.2passeasy.com/dumps/712-50/

Money Back Guarantee

712-50 Practice Exam Features:

* 712-50 Questions and Answers Updated Frequently

* 712-50 Practice Questions Verified by Expert Senior Certified Staff

* 712-50 Most Realistic Questions that Guarantee you a Pass on Your FirstTry

* 712-50 Practice Test Questions in Multiple Choice Formats and Updatesfor 1 Year