Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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

NEW QUESTION 1
- (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 2
- (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 3
- (Exam Topic 6)
When obtaining new products and services, why is it essential to collaborate with lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others?

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

Answer: D

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

NEW QUESTION 4
- (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 5
- (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 6
- (Exam Topic 6)
Who is responsible for verifying that audit directives are implemented?

A. IT Management
B. Internal Audit
C. IT Security
D. BOD Audit Committee

Answer: B

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

NEW QUESTION 7
- (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 8
- (Exam Topic 6)
In defining a strategic security plan for an organization, what should a CISO first analyze?

A. Reach out to a business similar to yours and ask for their plan
B. Set goals that are difficult to attain to drive more productivity
C. Review business acquisitions for the past 3 years
D. Analyze the broader organizational strategic plan

Answer: D

Explanation:
Reference: https://securityintelligence.com/the-importance-of-building-an-information-security-strategic-plan/

NEW QUESTION 9
- (Exam Topic 6)
Which of the following is the MOST effective method to counter phishing attacks?

A. User awareness and training
B. Host based Intrusion Detection System (IPS)
C. Acceptable use guide signed by all system users
D. Antispam solution

Answer: A

Explanation:
Reference: https://aware.eccouncil.org/4-best-ways-to-stop-phishing-with-security-awareness.html

NEW QUESTION 10
- (Exam Topic 6)
A Security Operations (SecOps) Manager is considering implementing threat hunting to be able to make better decisions on protecting information and assets. What is the MAIN goal of threat hunting to the SecOps Manager?

A. Improve discovery of valid detected events
B. Enhance tuning of automated tools to detect and prevent attacks
C. Replace existing threat detection strategies
D. Validate patterns of behavior related to an attack

Answer: A

Explanation:
Reference:
https://www.techtarget.com/searchsecurity/feature/7-SecOps-roles-and-responsibilities-for-the-modern-enterpris

NEW QUESTION 10
- (Exam Topic 2)

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

Answer: A

NEW QUESTION 11
- (Exam Topic 2)
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.

Answer: C

NEW QUESTION 12
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 15
- (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 18
- (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 22
- (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 23
- (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 26
- (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 27
- (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 32
- (Exam Topic 1)
Which of the following is a MAJOR consideration when an organization retains sensitive customer data and uses this data to better target the organization's products and services?

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

Answer: D

NEW QUESTION 35
- (Exam Topic 1)
One of the MAIN goals of a Business Continuity Plan is to

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

Answer: C

NEW QUESTION 39
- (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 41
- (Exam Topic 1)
Which of the following is a weakness of an asset or group of assets that can be exploited by one or more threats?

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

Answer: B

NEW QUESTION 42
- (Exam Topic 1)
What is the definition of Risk in Information Security?

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

Answer: A

NEW QUESTION 43
- (Exam Topic 1)
The PRIMARY objective for information security program development should be:

A. Reducing the impact of the risk to the business.
B. Establishing strategic alignment with bunsiness continuity requirements
C. Establishing incident response programs.
D. Identifying and implementing the best security solutions.

Answer: A

NEW QUESTION 48
- (Exam Topic 1)
What is a difference from the list below between quantitative and qualitative Risk Assessment?

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

Answer: A

NEW QUESTION 49
- (Exam Topic 1)
Which of the following most commonly falls within the scope of an information security governance steering committee?

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

Answer: D

NEW QUESTION 53
- (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 57
- (Exam Topic 1)
The Information Security Governance program MUST:

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

Answer: A

NEW QUESTION 60
- (Exam Topic 1)
An organization’s firewall technology needs replaced. A specific technology has been selected that is less costly than others and lacking in some important capabilities. The security officer has voiced concerns about sensitive data breaches but the decision is made to purchase. What does this selection indicate?

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

Answer: D

NEW QUESTION 63

- (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 67
- (Exam Topic 1)
Information security policies should be reviewed:

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

Answer: A

NEW QUESTION 72
- (Exam Topic 1)
According to ISO 27001, of the steps for establishing an Information Security Governance program listed below, which comes first?

A. Identify threats, risks, impacts and vulnerabilities
B. Decide how to manage risk
C. Define the budget of the Information Security Management System
D. Define Information Security Policy

Answer: D

NEW QUESTION 74
- (Exam Topic 1)
A global retail company is creating a new compliance management process. Which of the following regulations is of MOST importance to be tracked and managed by this process?

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

Answer: C

NEW QUESTION 75
- (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 78
- (Exam Topic 1)
From an information security perspective, information that no longer supports the main purpose of the business should be:

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

Answer: D

NEW QUESTION 82
- (Exam Topic 1)
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it

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

Answer: B

NEW QUESTION 84
- (Exam Topic 1)
The success of the Chief Information Security Officer is MOST dependent upon:

A. favorable audit findings
B. following the recommendations of consultants and contractors
C. development of relationships with organization executives
D. raising awareness of security issues with end users

Answer: C

NEW QUESTION 85
- (Exam Topic 1)
An organization's Information Security Policy is of MOST importance because

A. it communicates management’s commitment to protecting information resources
B. it is formally acknowledged by all employees and vendors
C. it defines a process to meet compliance requirements
D. it establishes a framework to protect confidential information

Answer: A

NEW QUESTION 89
- (Exam Topic 1)
Payment Card Industry (PCI) compliance requirements are based on what criteria?

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

Answer: D

NEW QUESTION 94
- (Exam Topic 1)
Which of the following are the MOST important factors for proactively determining system vulnerabilities?

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

Answer: D

NEW QUESTION 97
- (Exam Topic 1)
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

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

Answer: B

NEW QUESTION 100
- (Exam Topic 1)
Which of the following functions MUST your Information Security Governance program include for formal organizational reporting?

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

Answer: A

NEW QUESTION 103
- (Exam Topic 1)
When an organization claims it is secure because it is PCI-DSS certified, what is a good first question to ask towards assessing the effectiveness of their security program?

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

Answer:

C

NEW QUESTION 107
- (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 109
- (Exam Topic 6)
When information security falls under the Chief Information Officer (CIO), what is their MOST essential role?

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

Answer: D

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

NEW QUESTION 112
- (Exam Topic 6)
With a focus on the review and approval aspects of board responsibilities, the Data Governance Council recommends that the boards provide strategic oversight regarding information and information security, include these four things:

A. Metrics tracking security milestones, understanding criticality of information and information security, visibility into the types of information and how it is used, endorsement by the board of directors
B. Annual security training for all employees, continual budget reviews, endorsement of the development and implementation of a security program, metrics to track the program
C. Understanding criticality of information and information security, review investment in information security, endorse development and implementation of a security program, and require regular reports on adequacy and effectiveness
D. Endorsement by the board of directors for security program, metrics of security program milestones, annual budget review, report on integration and acceptance of program

Answer: C

Explanation:
Reference: https://nanopdf.com/download/information-security-governance-guidance-for-boards-of_pdf (9)

NEW QUESTION 116
- (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 118
- (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 122
- (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 127
- (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 132
- (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 134
- (Exam Topic 5)
What is the primary reason for performing a return on investment analysis?

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

Answer: B

NEW QUESTION 136
- (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 139
- (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 143
- (Exam Topic 5)
What are the three hierarchically related aspects of strategic planning and in which order should they be done?

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

Answer: D

NEW QUESTION 148
- (Exam Topic 5)
When analyzing and forecasting a capital expense budget what are not included?

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

Answer: A

NEW QUESTION 150
- (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 155
- (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 156
- (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 161
- (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 162
- (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 164
- (Exam Topic 5)
Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates.
What is one proven method to account for common elements found within separate regulations and/or standards?

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

Answer: D

NEW QUESTION 168
- (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 172
- (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 177
- (Exam Topic 5)
Which of the following defines the boundaries and scope of a risk assessment?

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

Answer: B

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

NEW QUESTION 181
- (Exam Topic 5)
John is the project manager for a large project in his organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can John do in this instance?

A. Refer the vendor to the Service Level Agreement (SLA) and insist that they make the changes.
B. Review the Request for Proposal (RFP) for guidance.
C. Withhold the vendor's payments until the issue is resolved.
D. Refer to the contract agreement for direction.

Answer: D

NEW QUESTION 185
- (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 190
- (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 195
- (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 198
- (Exam Topic 5)
SCENARIO: Critical servers show signs of erratic behavior within your organization's intranet. Initial information indicates the systems are under attack from an outside entity. As the Chief Information Security Officer (CISO), you decide to deploy the Incident Response Team (IRT) to determine the details of this incident and take action according to the information available to the team.
During initial investigation, the team suspects criminal activity but cannot initially prove or disprove illegal actions. What is the MOST critical aspect of the team's activities?

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

Answer: D

NEW QUESTION 201
- (Exam Topic 5)
File Integrity Monitoring (FIM) is considered a

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

Answer: C

NEW QUESTION 206
- (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 210
- (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 213
- (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 216
- (Exam Topic 5)
When creating contractual agreements and procurement processes why should security requirements be included?

A. To make sure they are added on after the process is completed
B. To make sure the costs of security is included and understood
C. To make sure the security process aligns with the vendor's security process
D. To make sure the patching process is included with the costs

Answer: B

NEW QUESTION 221
- (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 224
- (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.
Which of the following is the FIRST action the CISO will perform after receiving the audit report?

A. Inform peer executives of the audit results
B. Validate gaps and accept or dispute the audit findings
C. Create remediation plans to address program gaps
D. Determine if security policies and procedures are adequate

Answer: B

NEW QUESTION 226
- (Exam Topic 5)
Which of the following is the MOST important reason for performing assessments of the security portfolio?

A. To assure that the portfolio is aligned to the needs of the broader organization
B. To create executive support of the portfolio
C. To discover new technologies and processes for implementation within the portfolio

D. To provide independent 3rd party reviews of security effectiveness

Answer: A

NEW QUESTION 227
- (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 229
- (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 234
- (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 235
- (Exam Topic 5)
Which technology can provide a computing environment without requiring a dedicated hardware backend?

A. Mainframe server
B. Virtual Desktop
C. Thin client
D. Virtual Local Area Network

Answer: B

NEW QUESTION 239
- (Exam Topic 4)
Your penetration testing team installs an in-line hardware key logger onto one of your network machines. Which of the following is of major concern to the security organization?

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

Answer: C

NEW QUESTION 242
- (Exam Topic 5)
Which of the following best describes an access control process that confirms the identity of the entity seeking access to a logical or physical area?

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

Answer: B

NEW QUESTION 244

- (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 245
- (Exam Topic 4)
In terms of supporting a forensic investigation, it is now imperative that managers, first-responders, etc., accomplish the following actions to the computer under investigation:

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

Answer: B

NEW QUESTION 248
- (Exam Topic 4)
The process of creating a system which divides documents based on their security level to manage access to private data is known as

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

Answer: C

NEW QUESTION 252
- (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 253
- (Exam Topic 4)
Physical security measures typically include which of the following components?

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

Answer: A

NEW QUESTION 258
- (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 259
- (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 264
- (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 268
- (Exam Topic 4)
Which of the following backup sites takes the longest recovery time?

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

Answer: A

NEW QUESTION 272
- (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 276
- (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 277
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 278
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 280
- (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 282
- (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 284
- (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 285
- (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 288
- (Exam Topic 3)
Which of the following is critical in creating a security program aligned with an organization's goals?

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

Answer: B

NEW QUESTION 289
- (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 291
- (Exam Topic 3)
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

Answer: D

NEW QUESTION 292
- (Exam Topic 3)
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

Answer: A

NEW QUESTION 293
- (Exam Topic 3)
Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

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

Answer: A

NEW QUESTION 298
- (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 299
- (Exam Topic 3)
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

Answer: B

NEW QUESTION 300
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 305
- (Exam Topic 2)
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

Answer: D

NEW QUESTION 310
- (Exam Topic 2)

Which of the following best represents a calculation for Annual Loss Expectancy (ALE)?

A. Single loss expectancy multiplied by the annual rate of occurrence
B. Total loss expectancy multiplied by the total loss frequency
C. Value of the asset multiplied by the loss expectancy
D. Replacement cost multiplied by the single loss expectancy

Answer: A

NEW QUESTION 313
- (Exam Topic 2)
Which of the following best describes the purpose of the International Organization for Standardization (ISO) 27002 standard?

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

Answer: D

NEW QUESTION 317
- (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 319
- (Exam Topic 2)
Which of the following BEST describes an international standard framework that is based on the security model Information Technology—Code of Practice for Information Security Management?

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

Answer: A

NEW QUESTION 323
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 325
- (Exam Topic 2)
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

Answer: B

NEW QUESTION 329
- (Exam Topic 2)
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.

Answer: A

NEW QUESTION 333
- (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 336
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 338
- (Exam Topic 2)
Which of the following activities results in change requests?

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

Answer: C

NEW QUESTION 339
- (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 343
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 344
- (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 347
- (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 352
- (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 354
- (Exam Topic 2)
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

Answer: C

NEW QUESTION 358
.....

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