Exam Questions 712-50

EC-Council Certified CISO (CCISO)

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

NEW QUESTION 1
- (Exam Topic 6)
An organization has decided to develop an in-house BCM capability. The organization has determined it is best to follow a BCM standard published by the International Organization for Standardization (ISO).
The BEST ISO standard to follow that outlines the complete lifecycle of BCM is?

A. ISO 22318 Supply Chain Continuity
B. ISO 27031 BCM Readiness
C. ISO 22301 BCM Requirements
D. ISO 22317 BIA

Answer: C

Explanation:
Reference: https://www.smartsheet.com/content/iso-22301-business-continuity-guide

NEW QUESTION 2
- (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 3
- (Exam Topic 6)
Devising controls for information security is a balance between?

A. Governance and compliance
B. Auditing and security
C. Budget and risk tolerance
D. Threats and vulnerabilities

Answer: C

Explanation:
Reference: https://www.cybok.org/media/downloads/cybok_version_1.0.pdf

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)
From the CISO's perspective in looking at financial statements, the statement of retained earnings of an organization:

A. Has a direct correlation with the CISO's budget
B. Represents, in part, the savings generated by the proper acquisition and implementation of security controls
C. Represents the sum of all capital expenditures
D. Represents the percentage of earnings that could in part be used to finance future security controls

Answer: D

Explanation:
Reference: https://www.investopedia.com/terms/s/statement-of-retained-earnings.asp

NEW QUESTION 6
- (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 7
- (Exam Topic 6)
The main purpose of the SOC is:

A. An organization which provides Tier 1 support for technology issues and provides escalation when needed
B. A distributed organization which provides intelligence to governments and private sectors on cyber-criminal activities
C. The coordination of personnel, processes and technology to identify information security events and provide timely response and remediation
D. A device which consolidates event logs and provides real-time analysis of security alerts generated by applications and network hardware

Answer: C

Explanation:
Reference: https://www.eccouncil.org/what-is-soc/

NEW QUESTION 8
- (Exam Topic 6)
What organizational structure combines the functional and project structures to create a hybrid of the two?

A. Traditional
B. Composite
C. Project
D. Matrix

Answer: D

Explanation:
Reference: https://www.knowledgehut.com/tutorials/project-management/organization-structures

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)
When performing a forensic investigation, what are the two MOST common data sources for obtaining evidence from a computer and mobile devices?

A. RAM and unallocated space
B. Unallocated space and RAM
C. Slack space and browser cache
D. Persistent and volatile data

Answer: D

Explanation:
Reference: https://study.com/academy/lesson/data-storage-formats-digital-forensics-devices-types.html

NEW QUESTION 10
- (Exam Topic 6)
When managing a project, the MOST important activity in managing the expectations of stakeholders is:

A. To force stakeholders to commit ample resources to support the project
B. To facilitate proper communication regarding outcomes
C. To assure stakeholders commit to the project start and end dates in writing
D. To finalize detailed scope of the project at project initiation

Answer: B

Explanation:
Reference:
https://www.greycampus.com/blog/project-management/stakeholder-management-what-is-it-and-why-is-it-so-im

NEW QUESTION 13
- (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 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 18
- (Exam Topic 2)
A Chief Information Security Officer received a list of high, medium, and low impact audit findings. Which of the following represents the BEST course of action?

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

Answer: C

NEW QUESTION 22
- (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 26
- (Exam Topic 2)
Control Objectives for Information and Related Technology (COBIT) is which of the following?

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

Answer: C

NEW QUESTION 27
- (Exam Topic 2)
Which of the following are necessary to formulate responses to external audit findings?

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

Answer: C

NEW QUESTION 31
- (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 36
- (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 39
- (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 44
- (Exam Topic 1)
When managing the security architecture for your company you must consider:

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

Answer: D

NEW QUESTION 45
- (Exam Topic 1)
Developing effective security controls is a balance between:

A. Risk Management and Operations
B. Corporate Culture and Job Expectations
C. Operations and Regulations
D. Technology and Vendor Management

Answer: A

NEW QUESTION 50
- (Exam Topic 1)
You have purchased a new insurance policy as part of your risk strategy. Which of the following risk strategy options have you engaged in?

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

Answer: C

NEW QUESTION 53
- (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 58
- (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 61
- (Exam Topic 1)
Within an organization's vulnerability management program, who has the responsibility to implement remediation actions?

A. Security officer
B. Data owner
C. Vulnerability engineer
D. System administrator

Answer: D

NEW QUESTION 65
- (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 68
- (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 71
- (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 75
- (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 77
- (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 79
- (Exam Topic 1)
The alerting, monitoring and life-cycle management of security related events is typically handled by the

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

Answer: A

NEW QUESTION 82
- (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 84
- (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 85
- (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 89
- (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 93
- (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 95

- (Exam Topic 1)
Which of the following is considered the MOST effective tool against social engineering?

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

Answer: D

NEW QUESTION 96
- (Exam Topic 1)
When dealing with a risk management process, asset classification is important because it will impact the overall:

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

Answer: C

NEW QUESTION 97
- (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 98
- (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 100
- (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 103
- (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 108
- (Exam Topic 1)
If your organization operates under a model of "assumption of breach", you should:

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

Answer: C

NEW QUESTION 112
- (Exam Topic 1)
Regulatory requirements typically force organizations to implement

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

Answer: A

NEW QUESTION 114
- (Exam Topic 1)
In which of the following cases, would an organization be more prone to risk acceptance vs. risk mitigation?

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

Answer: C

NEW QUESTION 118
- (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 120
- (Exam Topic 1)
A security manager has created a risk program. Which of the following is a critical part of ensuring the program is successful?

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

Answer: A

NEW QUESTION 123
- (Exam Topic 1)
When managing an Information Security Program, which of the following is of MOST importance in order to influence the culture of an organization?

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

Answer: B

NEW QUESTION 128
- (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 132
- (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 135
- (Exam Topic 6)
Many successful cyber-attacks currently include:

A. Phishing Attacks
B. Misconfigurations
C. Social engineering
D. All of these

Answer: C

Explanation:
Reference: https://www.eccouncil.org/what-is-social-engineering/

NEW QUESTION 140
- (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 142
- (Exam Topic 6)
You are the CISO for an investment banking firm. The firm is using artificial intelligence (AI) to assist in approving clients for loans.
Which control is MOST important to protect AI products?

A. Hash datasets
B. Sanitize datasets
C. Delete datasets
D. Encrypt datasets

Answer: D

NEW QUESTION 146
- (Exam Topic 6)
Which of the following statements below regarding Key Performance indicators (KPIs) are true?

A. Development of KPI's are most useful when done independently
B. They are a strictly quantitative measure of success
C. They should be standard throughout the organization versus domain-specific so they are more easily correlated
D. They are a strictly qualitative measure of success

Answer: A

Explanation:
Reference: https://kpi.org/KPI-Basics/KPI-Development

NEW QUESTION 150
- (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 152
- (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 153
- (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 158
- (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 163
- (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 165
- (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. Compliance centric agenda
B. IT security centric agenda
C. Lack of risk management process
D. Lack of sponsorship from executive management

Answer: B

NEW QUESTION 168
- (Exam Topic 5)
Which of the following is MOST useful when developing a business case for security initiatives?

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

Answer: C

NEW QUESTION 170
- (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 175
- (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 discovers the scalability issue will only impact a small number of network segments. What is the next logical step to ensure the proper application of risk management methodology within the two-facto implementation project?

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

Answer: B

NEW QUESTION 180
- (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.
In what phase of the response will the team extract information from the affected systems without altering original data?

A. Response
B. Investigation
C. Recovery
D. Follow-up

Answer: B

NEW QUESTION 183
- (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 185
- (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 189
- (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 192
- (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 193
- (Exam Topic 5)
Which of the following is used to lure attackers into false environments so they can be monitored, contained, or blocked from reaching critical systems?

A. Segmentation controls.
B. Shadow applications.
C. Deception technology.
D. Vulnerability management.

Answer: B

NEW QUESTION 196
- (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 197
- (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 200
- (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. This global retail company is expected to accept credit card payments. Which of the following is of MOST concern when defining a security program for this organization?

A. International encryption restrictions
B. Compliance to Payment Card Industry (PCI) data security standards
C. Compliance with local government privacy laws
D. Adherence to local data breach notification laws

Answer: B

NEW QUESTION 202
- (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 203
- (Exam Topic 5)
The formal certification and accreditation process has four primary steps, what are they?

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

Answer: A

NEW QUESTION 208
- (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 209
- (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.
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 214
- (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 218
- (Exam Topic 5)
Which of the following best describes a portfolio?

A. The portfolio is used to manage and track individual projects
B. The portfolio is used to manage incidents and events
C. A portfolio typically consists of several programs
D. A portfolio delivers one specific service or program to the business

Answer: C

NEW QUESTION 221
- (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 226
- (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 228
- (Exam Topic 5)
A newly-hired CISO needs to understand the organization's financial management standards for business units and operations. Which of the following would be the best source of this information?

A. The internal accounting department

B. The Chief Financial Officer (CFO)
C. The external financial audit service
D. The managers of the accounts payables and accounts receivables teams

Answer: D

NEW QUESTION 231
- (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 232
- (Exam Topic 5)
What are the primary reasons for the development of a business case for a security project?

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

Answer: C

NEW QUESTION 234
- (Exam Topic 5)
As the Business Continuity Coordinator of a financial services organization, you are responsible for ensuring assets are recovered timely in the event of a disaster. Which is the BEST Disaster Recovery performance indicator to validate that you are prepared for a disaster?

A. Recovery Point Objective (RPO)
B. Disaster Recovery Plan
C. Recovery Time Objective (RTO)
D. Business Continuity Plan

Answer: D

Explanation:
Reference: https://www.resolver.com/resource/bcdr-metrics-that-matter/

NEW QUESTION 237
- (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 241
- (Exam Topic 5)
When dealing with risk, the information security practitioner may choose to:

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

Answer: C

NEW QUESTION 244
- (Exam Topic 5)
Simon had all his systems administrators implement hardware and software firewalls to ensure network security. They implemented IDS/IPS systems throughout the network to check for and stop any unauthorized traffic that may attempt to enter. Although Simon and his administrators believed they were secure, a hacker group was able to get into the network and modify files hosted on the company's website. After searching through the firewall and server logs, no one could find how the attackers were able to get in. He decides that the entire network needs to be monitored for critical and essential file changes. This monitoring tool alerts administrators when a critical file is altered. What tool could Simon and his administrators implement to accomplish this?

A. They need to use Nessus.
B. They can implement Wireshark.

C. Snort is the best tool for their situation.
D. They could use Tripwire.

Answer: C

Explanation:
Reference: https://searchnetworking.techtarget.com/definition/Snort

NEW QUESTION 245
- (Exam Topic 5)
Scenario: Your corporate systems have been under constant probing and attack from foreign IP addresses for more than a week. Your security team and security infrastructure have performed well under the stress. You are confident that your defenses have held up under the test, but rumors are spreading that sensitive customer data has been stolen and is now being sold on the Internet by criminal elements. During your investigation of the rumored compromise you discover that data has been breached and you have discovered the repository of stolen data on a server located in a foreign country. Your team now has full access to the data on the foreign server.
Your defenses did not hold up to the test as originally thought. As you investigate how the data was compromised through log analysis you discover that a hardworking, but misguided business intelligence analyst posted the data to an obfuscated URL on a popular cloud storage service so they could work on it from home during their off-time. Which technology or solution could you deploy to prevent employees from removing corporate data from your network? Choose the BEST answer.

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

Answer: B

NEW QUESTION 249
- (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 250
- (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 252
- (Exam Topic 5)
Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?

A. ITIL
B. Privacy Act
C. Sarbanes Oxley
D. PCI-DSS

Answer: B

NEW QUESTION 256
- (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 260
- (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 262
- (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 formulating the remediation plan, what is a required input?

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

Answer: B

NEW QUESTION 265
- (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 268
- (Exam Topic 5)
Which of the following is an accurate statement regarding capital expenses?

A. They are easily reduced through the elimination of usage, such as reducing power for lighting of work areas during off-hours
B. Capital expenses can never be replaced by operational expenses
C. Capital expenses are typically long-term investments with value being realized through their use
D. The organization is typically able to regain the initial cost by selling this type of asset

Answer: A

NEW QUESTION 271
- (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 273
- (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 277
- (Exam Topic 4)
Your organization provides open guest wireless access with no captive portals. What can you do to assist with law enforcement investigations if one of your guests is suspected of committing an illegal act using your network?

A. Configure logging on each access point
B. Install a firewall software on each wireless access point.
C. Provide IP and MAC address
D. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.

Answer: C

NEW QUESTION 281
- (Exam Topic 4)
One of your executives needs to send an important and confidential email. You want to ensure that the message cannot be read by anyone but the recipient. Which of the following keys should be used to encrypt the message?

A. Your public key
B. The recipient's private key
C. The recipient's public key
D. Certificate authority key

Answer: C

NEW QUESTION 284
- (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 289
- (Exam Topic 4)
A customer of a bank has placed a dispute on a payment for a credit card account. The banking system uses digital signatures to safeguard the integrity of their transactions. The bank claims that the system shows proof that the customer in fact made the payment. What is this system capability commonly known as?

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

Answer: A

NEW QUESTION 291
- (Exam Topic 4)
Which of the following is a countermeasure to prevent unauthorized database access from web applications?

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

Answer: C

NEW QUESTION 294
- (Exam Topic 4)
The general ledger setup function in an enterprise resource package allows for setting accounting periods. Access to this function has been permitted to users in finance, the shipping department, and production scheduling. What is the most likely reason for such broad access?

A. The need to change accounting periods on a regular basis.
B. The requirement to post entries for a closed accounting period.
C. The need to create and modify the chart of accounts and its allocations.
D. The lack of policies and procedures for the proper segregation of duties.

Answer: D

NEW QUESTION 295
- (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 299
- (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 302
- (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 307
- (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 309
- (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 312
- (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 317
- (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 321
- (Exam Topic 3)
You are the CISO of a commercial social media organization. The leadership wants to rapidly create new methods of sharing customer data through creative linkages with mobile devices. You have voiced concern about privacy regulations but the velocity of the business is given priority. Which of the following BEST describes this organization?

A. Risk averse
B. Risk tolerant
C. Risk conditional
D. Risk minimal

Answer: B

NEW QUESTION 324
- (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 328
- (Exam Topic 3)
As the CISO for your company you are accountable for the protection of information resources commensurate with:

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

Answer: D

NEW QUESTION 331
- (Exam Topic 3)
When is an application security development project complete?

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

Answer: A

NEW QUESTION 335
- (Exam Topic 3)
The Security Operations Center (SOC) just purchased a new intrusion prevention system (IPS) that needs to be deployed in-line for best defense. The IT group is concerned about putting the new IPS in-line because it might negatively impact network availability. What would be the BEST approach for the CISO to reassure the IT group?

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

Answer: D

NEW QUESTION 339
- (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 340

- (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 341
- (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 345
- (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 350
- (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 355
- (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 356
- (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 361
- (Exam Topic 3)
A CISO implements smart cards for credential management, and as a result has reduced costs associated with help desk operations supporting password resets. This demonstrates which of the following principles?

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

Answer: A

NEW QUESTION 366
- (Exam Topic 3)
Which of the following information may be found in table top exercises for incident response?

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

Answer: B

NEW QUESTION 369
- (Exam Topic 3)
Which of the following is MOST beneficial in determining an appropriate balance between uncontrolled innovation and excessive caution in an organization?

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

Answer: A

NEW QUESTION 373
- (Exam Topic 3)
Risk appetite is typically determined by which of the following organizational functions?

A. Security
B. Business units
C. Board of Directors
D. Audit and compliance

Answer: C

NEW QUESTION 378
- (Exam Topic 3)
Which of the following is the BEST indicator of a successful project?

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

Answer: D

NEW QUESTION 382
- (Exam Topic 3)
Which one of the following BEST describes which member of the management team is accountable for the day-to-day operation of the information security program?

A. Security administrators
B. Security mangers
C. Security technicians
D. Security analysts

Answer: B

NEW QUESTION 387
- (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 388
- (Exam Topic 3)
The company decides to release the application without remediating the high-risk vulnerabilities. Which of the following is the MOST likely reason for the company to release the application?

A. The company lacks a risk management process

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

Answer: C

NEW QUESTION 389
- (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 392
- (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 395
- (Exam Topic 3)
When managing the critical path of an IT security project, which of the following is MOST important?

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

Answer: D

NEW QUESTION 396
- (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 398
- (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 399
- (Exam Topic 2)
Which of the following are primary concerns for management with regard to assessing internal control objectives?

A. Confidentiality, Availability, Integrity
B. Compliance, Effectiveness, Efficiency
C. Communication, Reliability, Cost
D. Confidentiality, Compliance, Cost

Answer: B

NEW QUESTION 401

- (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 406
- (Exam Topic 2)
As the new CISO at the company you are reviewing the audit reporting process and notice that it includes only detailed technical diagrams. What else should be in the reporting process?

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

Answer: A

NEW QUESTION 410
- (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 412
- (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 415
- (Exam Topic 2)
The remediation of a specific audit finding is deemed too expensive and will not be implemented. Which of the following is a TRUE statement?

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

Answer: C

NEW QUESTION 418
- (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 423
- (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 426
- (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 430
- (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 432
- (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 434
- (Exam Topic 2)
Which of the following illustrates an operational control process:

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

Answer: B

NEW QUESTION 439
- (Exam Topic 2)
A missing/ineffective security control is identified. Which of the following should be the NEXT step?

A. Perform an audit to measure the control formally
B. Escalate the issue to the IT organization
C. Perform a risk assessment to measure risk
D. Establish Key Risk Indicators

Answer: C

NEW QUESTION 442
- (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 446
- (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 451
- (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 454
- (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 455
- (Exam Topic 2)
An IT auditor has recently discovered that because of a shortage of skilled operations personnel, the security administrator has agreed to work one late night shift a week as the senior computer operator. The most appropriate course of action for the IT auditor is to:

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

Answer: A

NEW QUESTION 457
.....

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