

712-50 Dumps

EC-Council Certified CISO (CCISO)

<https://www.certleader.com/712-50-dumps.html>



NEW QUESTION 1

- (Exam Topic 6)

Which level of data destruction applies logical techniques to sanitize data in all user-addressable storage locations?

- A. Purge
- B. Clear
- C. Mangle
- D. Destroy

Answer: B

Explanation:

Reference:

<https://it.brown.edu/computing-policies/electronic-equipment-disposition-policy/data-removal-recommendations>

NEW QUESTION 2

- (Exam Topic 6)

The primary responsibility for assigning entitlements to a network share lies with which role?

- A. CISO
- B. Data owner
- C. Chief Information Officer (CIO)
- D. Security system administrator

Answer: B

Explanation:

Reference: <https://resources.infosecinstitute.com/certification/data-and-system-ownership/>

NEW QUESTION 3

- (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 4

- (Exam Topic 6)

During a cyber incident, which non-security personnel might be needed to assist the security team?

- A. Threat analyst, IT auditor, forensic analyst
- B. Network engineer, help desk technician, system administrator
- C. CIO, CFO, CSO
- D. Financial analyst, payroll clerk, HR manager

Answer: A

NEW QUESTION 5

- (Exam Topic 6)

Optical biometric recognition such as retina scanning provides access to facilities through reading the unique characteristics of a person's eye. However, authorization failures can occur with individuals who have?

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

Answer: A

NEW QUESTION 6

- (Exam Topic 6)

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 7

- (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 8

- (Exam Topic 6)

Which of the following strategies provides the BEST response to a ransomware attack?

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

Answer: B

NEW QUESTION 9

- (Exam Topic 6)

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

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

Answer: C

Explanation:

Reference:

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

NEW QUESTION 10

- (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 10

- (Exam Topic 6)

What key technology can mitigate ransomware threats?

- A. Use immutable data storage
- B. Phishing exercises
- C. Application of multiple end point anti-malware solutions
- D. Blocking use of wireless networks

Answer: A

Explanation:

Reference:

<https://cloud.google.com/blog/products/identity-security/5-pillars-of-protection-to-prevent-ransomware-attacks>

NEW QUESTION 15

- (Exam Topic 6)

Which of the following are the triple constraints of project management?

- A. Time, quality, and scope
- B. Cost, quality, and time
- C. Scope, time, and cost
- D. Quality, scope, and cost

Answer: C

Explanation:

Reference:

<https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%>

NEW QUESTION 18

- (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 20

- (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 21

- (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 25

- (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 28

- (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 30

- (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 34

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 36

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 38

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 39

- (Exam Topic 2)

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

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

Answer: D

NEW QUESTION 40

- (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 44

- (Exam Topic 1)

Which of the following is of MOST importance when security leaders of an organization are required to align security to influence the culture of an organization?

- A. Poses a strong technical background
- B. Understand all regulations affecting the organization
- C. Understand the business goals of the organization
- D. Poses a strong auditing background

Answer: C

NEW QUESTION 45

- (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 46

- (Exam Topic 1)

When dealing with Security Incident Response procedures, which of the following steps come FIRST when reacting to an incident?

- A. Escalation
- B. Recovery
- C. Eradication
- D. Containment

Answer: D

NEW QUESTION 51

- (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 53

- (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 56

- (Exam Topic 1)

Which of the following represents the HIGHEST negative impact resulting from an ineffective security governance program?

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

Answer: D

NEW QUESTION 58

- (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 62

- (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 63

- (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 65

- (Exam Topic 1)

Which of the following is MOST important when dealing with an Information Security Steering committee:

- A. Include a mix of members from different departments and staff levels.
- B. Ensure that security policies and procedures have been vetted and approved.
- C. Review all past audit and compliance reports.
- D. Be briefed about new trends and products at each meeting by a vendor.

Answer: C

NEW QUESTION 66

- (Exam Topic 1)

What is the first thing that needs to be completed in order to create a security program for your organization?

- A. Risk assessment
- B. Security program budget
- C. Business continuity plan
- D. Compliance and regulatory analysis

Answer: A

NEW QUESTION 68

- (Exam Topic 1)

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

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

Answer: C

NEW QUESTION 71

- (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 72

- (Exam Topic 1)

You have a system with 2 identified risks. You determine the probability of one risk occurring is higher than the

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

Answer: C

NEW QUESTION 74

- (Exam Topic 1)

Which of the following intellectual Property components is focused on maintaining brand recognition?

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

Answer: A

NEW QUESTION 78

- (Exam Topic 1)

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

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

Answer: D

NEW QUESTION 79

- (Exam Topic 1)

A global health insurance company is concerned about protecting confidential information. Which of the following is of MOST concern to this organization?

- A. Compliance to the Payment Card Industry (PCI) regulations.
- B. Alignment with financial reporting regulations for each country where they operate.
- C. Alignment with International Organization for Standardization (ISO) standards.
- D. Compliance with patient data protection regulations for each country where they operate.

Answer: D

NEW QUESTION 80

- (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 85

- (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 88

- (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 90

- (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 95

- (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 97

- (Exam Topic 1)

The framework that helps to define a minimum standard of protection that business stakeholders must attempt to achieve is referred to as a standard of:

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

Answer: B

NEW QUESTION 101

- (Exam Topic 1)

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

- A. Confidential/Protected Information
- B. Bodily Information
- C. Territorial Information
- D. Communications Information

Answer: A

NEW QUESTION 106

- (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 109

- (Exam Topic 1)

When briefing senior management on the creation of a governance process, the MOST important aspect should be:

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

Answer: D

NEW QUESTION 114

- (Exam Topic 1)

Quantitative Risk Assessments have the following advantages over qualitative risk assessments:

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

Answer:

A

NEW QUESTION 115

- (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 120

- (Exam Topic 1)

Why is it vitally important that senior management endorse a security policy?

- A. So that they will accept ownership for security within the organization.
- B. So that employees will follow the policy directives.
- C. So that external bodies will recognize the organizations commitment to security.
- D. So that they can be held legally accountable.

Answer: A

NEW QUESTION 125

- (Exam Topic 1)

Which of the following has the GREATEST impact on the implementation of an information security governance model?

- A. Organizational budget
- B. Distance between physical locations
- C. Number of employees
- D. Complexity of organizational structure

Answer: D

NEW QUESTION 126

- (Exam Topic 1)

Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:

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

Answer: D

NEW QUESTION 127

- (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 130

- (Exam Topic 1)

A security officer wants to implement a vulnerability scanning program. The officer is uncertain of the state of vulnerability resiliency within the organization's large IT infrastructure. What would be the BEST approach to minimize scan data output while retaining a realistic view of system vulnerability?

- A. Scan a representative sample of systems
- B. Perform the scans only during off-business hours
- C. Decrease the vulnerabilities within the scan tool settings
- D. Filter the scan output so only pertinent data is analyzed

Answer: A

NEW QUESTION 133

- (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 138

- (Exam Topic 1)

Which of the following provides an audit framework?

- A. Control Objectives for IT (COBIT)
- B. Payment Card Industry-Data Security Standard (PCI-DSS)
- C. International Organization Standard (ISO) 27002
- D. National Institute of Standards and Technology (NIST) SP 800-30

Answer: A

NEW QUESTION 141

- (Exam Topic 1)

What is the relationship between information protection and regulatory compliance?

- A. That all information in an organization must be protected equally.
- B. The information required to be protected by regulatory mandate does not have to be identified in the organizations data classification policy.
- C. That the protection of some information such as National ID information is mandated by regulation and other information such as trade secrets are protected based on business need.
- D. There is no relationship between the two.

Answer: C

NEW QUESTION 145

- (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 150

- (Exam Topic 1)

Who in the organization determines access to information?

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

Answer: C

NEW QUESTION 153

- (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 157

- (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 161

- (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 162

- (Exam Topic 6)

What are the common data hiding techniques used by criminals?

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

Answer: D

Explanation:

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

NEW QUESTION 164

- (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 165

- (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 168

- (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 170

- (Exam Topic 6)

As the CISO, you are the project sponsor for a highly visible log management project. The objective of the project is to centralize all the enterprise logs into a security information and event management (SIEM) system. You requested the results of the performance quality audits activity. The performance quality audit activity is done in what project management process group?

- A. Executing
- B. Controlling
- C. Planning
- D. Closing

Answer: A

Explanation:

Reference:

<https://blog.masterofproject.com/executing-process-group-project-management/#:~:text=Executing%20Process>

NEW QUESTION 174

- (Exam Topic 6)

What is a key policy that should be part of the information security plan?

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

Answer: C

Explanation:

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

NEW QUESTION 179

- (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 180

- (Exam Topic 5)

What is the primary reason for performing a return on investment analysis?

- A. To decide between multiple vendors
- B. To decide if 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 183

- (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 186

- (Exam Topic 5)

Scenario: Most industries require compliance with multiple government regulations and/or industry standards to meet data protection and privacy mandates. When multiple regulations or standards apply to your industry you should set controls to meet the:

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

Answer: C

NEW QUESTION 189

- (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 193

- (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 196

- (Exam Topic 5)

Which of the following provides an independent assessment of a vendor's internal security controls and overall posture?

- A. Alignment with business goals
- B. ISO27000 accreditation
- C. PCI attestation of compliance
- D. Financial statements

Answer: B

NEW QUESTION 197

- (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 199

- (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 204

- (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 209

- (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 214

- (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 218

- (Exam Topic 5)

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

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

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

Answer: C

NEW QUESTION 221

- (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 223

- (Exam Topic 5)

The newly appointed CISO of an organization is reviewing the IT security strategic plan. Which of the following is the MOST important component of the strategic plan?

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

Answer: B

NEW QUESTION 228

- (Exam Topic 5)

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

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

Answer: C

NEW QUESTION 233

- (Exam Topic 5)

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

Which of the following needs to be performed NEXT?

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

Answer: A

NEW QUESTION 235

- (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 238

- (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 242

- (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 246

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

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

Answer: B

NEW QUESTION 251

- (Exam Topic 5)

A large number of accounts in a hardened system were suddenly compromised to an external party. Which of the following is the MOST probable threat actor involved in this incident?

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

Answer: D

NEW QUESTION 254

- (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 257

- (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 261

- (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 266

- (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 271

- (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 274

- (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.

The CISO has been able to implement a number of technical controls and is able to influence the Information Technology teams but has not been able to influence the rest of the organization. From an organizational perspective, which of the following is the LIKELY reason for this?

- A. The CISO does not report directly to the CEO of the organization
- B. The CISO reports to the IT organization
- C. The CISO has not implemented a policy management framework
- D. The CISO has not implemented a security awareness program

Answer: B

NEW QUESTION 278

- (Exam Topic 5)

When updating the security strategic planning document what two items must be included?

- A. Alignment with the business goals and the vision of the CIO
- B. The risk tolerance of the company and the company mission statement
- C. The executive summary and vision of the board of directors
- D. The alignment with the business goals and the risk tolerance

Answer: D

NEW QUESTION 279

- (Exam Topic 5)

A CISO decides to analyze the IT infrastructure to ensure security solutions adhere to the concepts of how hardware and software is implemented and managed within the organization. Which of the following principles does this best demonstrate?

- A. Effective use of existing technologies
- B. Create a comprehensive security awareness program and provide success metrics to business units
- C. Proper budget management
- D. Leveraging existing implementations

Answer: B

NEW QUESTION 283

- (Exam Topic 5)

When project costs continually increase throughout implementation due to large or rapid changes in customer or user requirements, this is commonly known as:

- A. Cost/benefit adjustments
- B. Scope creep
- C. Prototype issues
- D. Expectations management

Answer: B

Explanation:

Reference:

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

NEW QUESTION 286

- (Exam Topic 5)

Which of the following conditions would be the MOST probable reason for a security project to be rejected by the executive board of an organization?

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

Answer: B

NEW QUESTION 288

- (Exam Topic 5)

Scenario: 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. Baselineing of computer systems
- D. Scanning for viruses

Answer: A

NEW QUESTION 291

- (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 296

- (Exam Topic 5)

The Annualized Loss Expectancy (Before) minus Annualized Loss Expectancy (After) minus Annual Safeguard Cost is the formula for determining:

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

Answer: B

NEW QUESTION 300

- (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 304

- (Exam Topic 5)

Bob waits near a secured door, holding a box. He waits until an employee walks up to the secured door and uses the special card in order to access the restricted area of the target company. Just as the employee opens the door, Bob walks up to the employee (still holding the box) and asks the employee to hold the door open so that he can enter. What is the best way to undermine the social engineering activity of tailgating?

- A. Post a sign that states, "no tailgating" next to the special card reader adjacent to the secure door
- B. Issue special cards to access secure doors at the company and provide a one-time only brief description of use of the special card
- C. Educate and enforce physical security policies of the company to all the employees on a regular basis
- D. Setup a mock video camera next to the special card reader adjacent to the secure door

Answer: C

NEW QUESTION 307

- (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 311

- (Exam Topic 5)

If a Virtual Machine's (VM) data is being replicated and that data is corrupted, this corruption will automatically be replicated to the other machine(s). What would be the BEST control to safeguard data integrity?

- A. Backup to tape
- B. Maintain separate VM backups
- C. Backup to a remote location
- D. Increase VM replication frequency

Answer: B

Explanation:

Reference:

<https://www.isaca.org/resources/isaca-journal/issues/2018/volume-1/is-audit-basics-backup-andrecovery>

NEW QUESTION 316

- (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 318

- (Exam Topic 5)

The total cost of security controls should:

- A. Be equal to the value of the information resource being protected
- B. Be greater than the value of the information resource being protected
- C. Be less than the value of the information resource being protected
- D. Should not matter, as long as the information resource is protected

Answer: C

NEW QUESTION 320

- (Exam Topic 5)

As the Chief Information Security Officer, you want to ensure data shared securely, especially when shared with third parties outside the organization. What protocol provides the ability to extend the network perimeter with the use of encapsulation and encryption?

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

Answer: D

Explanation:

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

NEW QUESTION 323

- (Exam Topic 5)

You are just hired as the new CISO and are being briefed on all the Information Security projects that your section has on going. You discover that most projects are behind schedule and over budget.

Using the best business practices for project management you determine that the project correct aligns with the company goals. What needs to be verified FIRST?

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

Answer: A

NEW QUESTION 328

- (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 332

- (Exam Topic 5)

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

- A. Annual Rate of Occurrence and Asset Value
- B. Single Loss Expectancy and Exposure Factor
- C. Safeguard Value and Annual Rate of Occurrence
- D. Annual Rate of Occurrence and Single Loss Expectancy

Answer: D

NEW QUESTION 337

- (Exam Topic 5)

Scenario: You are the CISO and are required to brief the C-level executive team on your information security audit for the year. During your review of the audit findings you discover that many of the controls that were put in place the previous year to correct some of the findings are not performing as needed. You have thirty days until the briefing.

To formulate a remediation plan for the non-performing controls what other document do you need to review before adjusting the controls?

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

Answer: A

NEW QUESTION 341

- (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 346

- (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 351

- (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 356

- (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 357

- (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 361

- (Exam Topic 4)

What type of attack requires the least amount of technical equipment and has the highest success rate?

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

Answer: C

NEW QUESTION 366

- (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 371

- (Exam Topic 4)

The process for identifying, collecting, and producing digital information in support of legal proceedings is called

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

Answer: B

NEW QUESTION 374

- (Exam Topic 4)

An anonymity network is a series of?

- A. Covert government networks
- B. War driving maps
- C. Government networks in Tora
- D. Virtual network tunnels

Answer: D

NEW QUESTION 375

- (Exam Topic 4)

While designing a secondary data center for your company what document needs to be analyzed to determine to how much should be spent on building the data center?

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

Answer: B

NEW QUESTION 378

- (Exam Topic 4)

SQL injection is a very popular and successful injection attack method. Identify the basic SQL injection text:

- A. ' o 1=1 -
- B. /./././././
- C. "DROPTABLE USERNAME"
- D. NOPS

Answer: A

NEW QUESTION 382

- (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 384

- (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 386

- (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 387

- (Exam Topic 4)

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

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

Answer: D

NEW QUESTION 389

- (Exam Topic 3)

Which of the following functions implements and oversees the use of controls to reduce risk when creating an information security program?

- A. Risk Assessment
- B. Incident Response
- C. Risk Management
- D. Network Security administration

Answer: C

NEW QUESTION 390

- (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 395

- (Exam Topic 3)

Knowing the potential financial loss an organization is willing to suffer if a system fails is a determination of which of the following?

- A. Cost benefit
- B. Risk appetite
- C. Business continuity
- D. Likelihood of impact

Answer: B

NEW QUESTION 399

- (Exam Topic 3)

Which of the following represents the best method of ensuring business unit alignment with security program requirements?

- A. Provide clear communication of security requirements throughout the organization
- B. Demonstrate executive support with written mandates for security policy adherence
- C. Create collaborative risk management approaches within the organization
- D. Perform increased audits of security processes and procedures

Answer: C

NEW QUESTION 403

- (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 405

- (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 409

- (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 412

- (Exam Topic 3)

A stakeholder is a person or group:

- A. Vested in the success and/or failure of a project or initiative regardless of budget implications.
- B. Vested in the success and/or failure of a project or initiative and is tied to the project budget.
- C. That has budget authority.
- D. That will ultimately use the system.

Answer: A

NEW QUESTION 414

- (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 416

- (Exam Topic 3)

Which of the following represents the BEST method of ensuring security program alignment to business needs?

- A. Create a comprehensive security awareness program and provide success metrics to business units
- B. Create security consortiums, such as strategic security planning groups, that include business unit participation
- C. Ensure security implementations include business unit testing and functional validation prior to production rollout
- D. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role

Answer: B

NEW QUESTION 421

- (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 managers
- C. Security technicians
- D. Security analysts

Answer: B

NEW QUESTION 424

- (Exam Topic 3)

When operating under severe budget constraints a CISO will have to be creative to maintain a strong security organization. Which example below is the MOST creative way to maintain a strong security posture during these difficult times?

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

Answer: C

NEW QUESTION 429

- (Exam Topic 3)

How often should the SSAE16 report of your vendors be reviewed?

- A. Quarterly
- B. Semi-annually
- C. Annually
- D. Bi-annually

Answer: C

NEW QUESTION 431

- (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 432

- (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 434

- (Exam Topic 3)

You currently cannot provide for 24/7 coverage of your security monitoring and incident response duties and your company is resistant to the idea of adding more full-time employees to the payroll. Which combination of solutions would help to provide the coverage needed without the addition of more dedicated staff? (choose the best answer):

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

Answer: B

NEW QUESTION 438

- (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 439

- (Exam Topic 3)

You manage a newly created Security Operations Center (SOC), your team is being inundated with security alerts and don't know what to do. What is the BEST approach to handle this situation?

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

Answer: B

NEW QUESTION 440

- (Exam Topic 3)

Which of the following is a major benefit of applying risk levels?

- A. Risk management governance becomes easier since most risks remain low once mitigated
- B. Resources are not wasted on risks that are already managed to an acceptable level
- C. Risk budgets are more easily managed due to fewer identified risks as a result of using a methodology
- D. Risk appetite can increase within the organization once the levels are understood

Answer: B

NEW QUESTION 443

- (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 444

- (Exam Topic 3)

A CISO has recently joined an organization with a poorly implemented security program. The desire is to base the security program on a risk management approach. Which of the following is a foundational requirement in order to initiate this type of program?

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

Answer: D

NEW QUESTION 449

- (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 453

- (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 455

- (Exam Topic 2)

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

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

Answer: A

NEW QUESTION 458

- (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 463

- (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 466

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 467

- (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 468

- (Exam Topic 2)

An organization is required to implement background checks on all employees with access to databases containing credit card information. This is considered a security

- A. Procedural control
- B. Management control
- C. Technical control
- D. Administrative control

Answer: B

NEW QUESTION 471

- (Exam Topic 2)

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

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

Answer: C

NEW QUESTION 472

- (Exam Topic 2)

Which of the following set of processes is considered to be one of the cornerstone cycles of the International Organization for Standardization (ISO) 27001 standard?

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

Answer: B

NEW QUESTION 477

- (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 482

- (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 486

- (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 491

- (Exam Topic 2)

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

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

Answer: B

NEW QUESTION 494

- (Exam Topic 2)

Which of the following reports should you as an IT auditor use to check on compliance with a service level agreement's requirement for uptime?

- A. Systems logs
- B. Hardware error reports
- C. Utilization reports
- D. Availability reports

Answer: D

NEW QUESTION 497

.....

Thank You for Trying Our Product

* 100% Pass or Money Back

All our products come with a 90-day Money Back Guarantee.

* One year free update

You can enjoy free update one year. 24x7 online support.

* Trusted by Millions

We currently serve more than 30,000,000 customers.

* Shop Securely

All transactions are protected by VeriSign!

100% Pass Your 712-50 Exam with Our Prep Materials Via below:

<https://www.certleader.com/712-50-dumps.html>