EC-COUNCIL.512-50.v2022-07-16.q140

Exam Code:	512-50
Exam Name:	EC-Council Information Security Manager (E|ISM)
Certification Provider:	EC-COUNCIL
Free Question Number:	140
Version:	v2022-07-16
# of views:	2244
# of Questions views:	1400
https://www.freepdfdumps.com/EC-COUNCIL.512-50.v2022-07-16.q140.html	

NEW QUESTION: 1
Your company has a "no right to privacy" notice on all logon screens for your information systems and users sign an Acceptable Use Policy informing them of this condition. A peer group member and friend comes to you and requests access to one of her employee's email account. What should you do? (choose the BEST answer):
A. Reset the employee's password and give it to the supervisor.
B. Assist her with the request, but only after her supervisor signs off on the action.
C. Grant her access, the employee has been adequately warned through the AUP.
D. Deny the request citing national privacy laws.
Answer: (SHOW ANSWER)

NEW QUESTION: 2
When choosing a risk mitigation method what is the MOST important factor?
A. Approval from the board of directors
B. Metrics of mitigation method success
C. Cost of the mitigation is less than the risk
D. Mitigation method complies with PCI regulations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 3
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 (LEAVE A REPLY)
Explanation
Scenario8

NEW QUESTION: 4
A recommended method to document the respective roles of groups and individuals for a given process is to:
A. Develop a telephone call tree for emergency response
B. Develop a detailed internal organization chart
C. Develop an isolinear response matrix with cost benefit analysis projections
D. Develop a Responsible, Accountable, Consulted, Informed (RACI) chart
Answer: (SHOW ANSWER)

NEW QUESTION: 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. Full off-site backup of every server
B. Pre-built servers and routers
C. Permanent alternative routing
D. Third-party emergency repair contract
Answer: C (LEAVE A REPLY)

NEW QUESTION: 6
Ensuring that the actions of a set of people, applications and systems follow the organization's rules is BEST described as:
A. Compliance management
B. Risk management
C. Mitigation management
D. Security management
Answer: A (LEAVE A REPLY)

NEW QUESTION: 7
Which of the following functions evaluates risk present in IT initiatives and/or systems when implementing an information security program?

A. Risk Assessment
B. System Testing
C. Risk Management
D. Vulnerability Assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 8
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 hardening standards
B. Lack of asset management processes
C. Lack of change management processes
D. Lack of proper access controls
Answer: (SHOW ANSWER)

NEW QUESTION: 9
A Security Operations Centre (SOC) manager is informed that a database containing highly sensitive corporate strategy information is under attack. Information has been stolen and the database server was disconnected.
Who must be informed of this incident?
A. All executive staff
B. Internal audit
C. Government regulators
D. The data owner
Answer: (SHOW ANSWER)

NEW QUESTION: 10
File Integrity Monitoring (FIM) is considered a
A. Network based security preventative control
B. Security detective control
C. Software segmentation control
D. User segmentation control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 11
Which of the following is critical in creating a security program aligned with an organization's goals?

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

NEW QUESTION: 12
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. Business charter
C. Penetration test agreement
D. Names and phone numbers of those who conducted the audit
Answer: A (LEAVE A REPLY)

NEW QUESTION: 13
The Information Security Governance program MUST:
A. integrate with other organizational governance processes
B. show a return on investment for the organization
C. integrate with other organizational governance processes
D. support user choice for Bring Your Own Device (BYOD)
Answer: (SHOW ANSWER)

NEW QUESTION: 14
Which of the following is MOST useful when developing a business case for security initiatives?
A. Request for proposals
B. Cost/benefit analysis
C. Budget forecasts
D. Vendor management
Answer: (SHOW ANSWER)

NEW QUESTION: 15
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: (SHOW ANSWER)

NEW QUESTION: 16
Which of the following are the MOST important factors for proactively determining system vulnerabilities?
A. Subscribe to vendor mailing list to get notification of system vulnerabilities
B. Deploy Intrusion Detection System (IDS) and install anti-virus on systems
C. Configure firewall, perimeter router and Intrusion Prevention System (IPS)
D. Conduct security testing, vulnerability scanning, and penetration testing
Answer: D (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 17
What is the FIRST step in developing the vulnerability management program?
A. Define Policy
B. Baseline the Environment
C. Organization Vulnerability
D. Maintain and Monitor
Answer: (SHOW ANSWER)

NEW QUESTION: 18
In accordance with best practices and international standards, how often is security awareness training provided to employees of an organization?
A. High risk environments 6 months, low risk environments 12 months
B. Every six months
C. Every 18 months
D. Every 12 months
Answer: D (LEAVE A REPLY)

NEW QUESTION: 19

The alerting, monitoring and life-cycle management of security related events is typically handled by the

A. governance, risk, and compliance tools

B. security threat and vulnerability management process

C. risk assessment process

D. risk management process

Answer: B (LEAVE A REPLY)

NEW QUESTION: 20

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

A. During the monthly review cycle

B. Immediately so the employee account(s) can be disabled

C. Before an audit

D. At the end of the day once the employee is off site

Answer: B (LEAVE A REPLY)

NEW QUESTION: 21

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

A. System hardening and patching requirements

B. Nonlinearities in physical security performance metrics

C. Anti-virus for mobile devices

D. Defense in depth cost enumerated costs

Answer: B (LEAVE A REPLY)

NEW QUESTION: 22

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: (SHOW ANSWER)

NEW QUESTION: 23

Who is responsible for securing networks during a security incident?

A. Chief Information Security Officer (CISO)

B. Disaster Recovery (DR) manager

C. Security Operations Center (SO

D. Incident Response Team (IRT)

Answer: D (LEAVE A REPLY)

NEW QUESTION: 24
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 delivers one specific service or program to the business
D. A portfolio typically consists of several programs
Answer: (SHOW ANSWER)

NEW QUESTION: 25
Which of the following is MOST likely to be discretionary?
A. Standards
B. Guidelines
C. Policies
D. Procedures
Answer: B (LEAVE A REPLY)

NEW QUESTION: 26
Which of the following organizations is typically in charge of validating the implementation and effectiveness of security controls?
A. Internal/External Audit
B. Security Administrators
C. Risk Management
D. Security Operations
Answer: A (LEAVE A REPLY)

NEW QUESTION: 27
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 compliance test of the program compiler controls
B. A compliance test of program library controls
C. A substantive test of program library controls
D. A substantive test of the program compiler controls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 28
Which of the following is the MOST important reason for performing assessments of the security portfolio?
A. To create executive support of the portfolio
B. To provide independent 3rd party reviews of security effectiveness

C. To discover new technologies and processes for implementation within the portfolio
D. To assure that the portfolio is aligned to the needs of the broader organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 29
Which of the following is the MAIN security concern for public cloud computing?
A. Unable to run anti-virus scans
B. Unable to track log on activity
C. Unable to patch systems as needed
D. Unable to control physical access to the servers
Answer: D (LEAVE A REPLY)

NEW QUESTION: 30
Which regulation or policy governs protection of personally identifiable user data gathered during a cyber investigation?
A. ITIL
B. PCI-DSS
C. Sarbanes Oxley
D. Privacy Act
Answer: (SHOW ANSWER)

NEW QUESTION: 31
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.
What type of control is being implemented by supervisors and data owners?
A. Technical
B. Administrative
C. Operational
D. Management
Answer: (SHOW ANSWER)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com

512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 32
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. Eradication of malware and system restoration
B. Regular communication of incident status to executives
C. Preservation of information
D. Determination of the attack source
Answer: (SHOW ANSWER)

NEW QUESTION: 33
As the CISO for your company you are accountable for the protection of information resources commensurate with:
A. Customer demand
B. Risk of exposure
C. Cost and time to replace
D. Insurability tables
Answer: B (LEAVE A REPLY)

NEW QUESTION: 34
When dealing with risk, the information security practitioner may choose to:
A. transfer
B. defer
C. assign
D. acknowledge
Answer: D (LEAVE A REPLY)

NEW QUESTION: 35
A global retail organization is looking to implement a consistent Disaster Recovery and Business Continuity Process across all of its business units. Which of the following standards and guidelines can BEST address this organization's need?
A. Information Technology Infrastructure Library (ITIL)

B. International Organization for Standardizations - 27005 (ISO-27005)
C. Payment Card Industry Data Security Standards (PCI-DSS)
D. International Organization for Standardizations - 22301 (ISO-22301)
Answer: D (LEAVE A REPLY)

NEW QUESTION: 36
Which of the following represents the BEST method of ensuring security program alignment to business needs?
A. Ensure security implementations include business unit testing and functional validation prior to production rollout
B. Create security consortiums, such as strategic security planning groups, that include business unit participation
C. Ensure the organization has strong executive-level security representation through clear sponsorship or the creation of a CISO role
D. Create a comprehensive security awareness program and provide success metrics to business units
Answer: B (LEAVE A REPLY)

NEW QUESTION: 37
Scenario: An organization has recently appointed a CISO. This is a new role in the organization and it signals the increasing need to address security consistently at the enterprise level. This new CISO, while confident with skills and experience, is constantly on the defensive and is unable to advance the IT security centric agenda.
Which of the following is the reason the CISO has not been able to advance the security agenda in this organization?
A. Lack of influence with leaders outside IT
B. Lack of a security awareness program
C. Lack of business continuity process
D. Lack of identification of technology stake holders
Answer: A (LEAVE A REPLY)

NEW QUESTION: 38
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. Provide IP and MAC address
B. Configure logging on each access point
C. Disable SSID Broadcast and enable MAC address filtering on all wireless access points.
D. Install a firewall software on each wireless access point.
Answer: (SHOW ANSWER)

NEW QUESTION: 39
When gathering security requirements for an automated business process improvement program, which of the following is MOST important?
A. Type of data contained in the process/system
B. Type of connection/protocol used to transfer the data
C. Type of encryption required for the data once it is at rest
D. Type of computer the data is processed on
Answer: A (LEAVE A REPLY)

NEW QUESTION: 40
Scenario: You are the CISO and have just completed your first risk assessment for your organization. You find many risks with no security controls, and some risks with inadequate controls. You assign work to your staff to create or adjust existing security controls to ensure they are adequate for risk mitigation needs.
When adjusting the controls to mitigate the risks, how often should the CISO perform an audit to verify the controls?
A. Semi-annually
B. Annually
C. Never
D. Quarterly
Answer: C (LEAVE A REPLY)

NEW QUESTION: 41
Which is the BEST solution to monitor, measure, and report changes to critical data in a system?
A. SNMP traps
B. Syslog
C. File integrity monitoring
D. Application logs
Answer: C (LEAVE A REPLY)

NEW QUESTION: 42
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. 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
B. Explain to the IT group that the IPS won't cause any network impact because it will fail open

C. Work with the IT group and tell them to put IPS in-line and say it won't cause any network impact
D. 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
Answer: A (LEAVE A REPLY)

NEW QUESTION: 43
If your organization operates under a model of "assumption of breach", you should:
A. Protect all information resource assets equally
B. Purchase insurance for your compliance liability
C. Focus your security efforts on high value assets
D. Establish active firewall monitoring protocols
Answer: (SHOW ANSWER)

NEW QUESTION: 44
The amount of risk an organization is willing to accept in pursuit of its mission is known as
A. Risk acceptance
B. Risk transfer
C. Risk mitigation
D. Risk tolerance
Answer: D (LEAVE A REPLY)

NEW QUESTION: 45
An organization has defined a set of standard security controls. This organization has also defined the circumstances and conditions in which they must be applied. What is the NEXT logical step in applying the controls in the organization?
A. Perform an asset classification
B. Analyze existing controls on systems
C. Determine the risk tolerance
D. Create an architecture gap analysis
Answer: A (LEAVE A REPLY)

NEW QUESTION: 46
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 is out of date and does not provide for a scalable solution across the enterprise
B. The security officer should allow time for the organization to get accustomed to her presence before initiating security projects

C. The software license expiration is probably out of synchronization with other software licenses
D. The project was initiated without an effort to get support from impacted business units in the organization
Answer: (SHOW ANSWER)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 47
When dealing with a risk management process, asset classification is important because it will impact the overall:
A. Risk treatment
B. Risk monitoring
C. Threat identification
D. Risk tolerance
Answer: A (LEAVE A REPLY)

NEW QUESTION: 48
What is the first thing that needs to be completed in order to create a security program for your organization?
A. Compliance and regulatory analysis
B. Business continuity plan
C. Security program budget
D. Risk assessment
Answer: D (LEAVE A REPLY)

NEW QUESTION: 49
Which of the following is considered a project versus a managed process?
A. continuous vulnerability assessment and vulnerability repair
B. monitoring external and internal environment during incident response
C. ongoing risk assessments of routine operations
D. installation of a new firewall system
Answer: D (LEAVE A REPLY)

NEW QUESTION: 50
Who in the organization determines access to information?
A. Legal department
B. Compliance officer
C. Information security officer
D. Data Owner
Answer: D (LEAVE A REPLY)

NEW QUESTION: 51
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 attempt to maintain power until investigators arrive
B. Secure the area.
C. Immediately place hard drive and other components in an anti-static bag
D. Secure the area and shut-down the computer until investigators arrive
Answer: (SHOW ANSWER)

NEW QUESTION: 52
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 (LEAVE A REPLY)
Reference: https://digitalguardian.com/blog/what-identity-and-access-management-iam

NEW QUESTION: 53
When deploying an Intrusion Prevention System (IPS) the BEST way to get maximum protection from the system is to deploy it
A. In-line and turn on alert mode to stop malicious traffic.
B. In-line and turn on blocking mode to stop malicious traffic.
C. In promiscuous mode and block malicious traffic.
D. In promiscuous mode and only detect malicious traffic.
Answer: (SHOW ANSWER)

NEW QUESTION: 54
The total cost of security controls should:
A. Be less than the value of the information resource being protected
B. Be greater than the value of the information resource being protected
C. Should not matter, as long as the information resource is protected
D. Be equal to the value of the information resource being protected

Answer: (SHOW ANSWER)

NEW QUESTION: 55
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. privacy protection
C. data classification
D. data security system
Answer: C (LEAVE A REPLY)

NEW QUESTION: 56
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. Identify and assess the risk assessment process used by management.
C. Identify information assets and the underlying systems.
D. Disclose the threats and impacts to management.
Answer: (SHOW ANSWER)

NEW QUESTION: 57
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 comply to industry regulations
B. In-line hardware keyloggers are undetectable by software
C. In-line hardware keyloggers are relatively inexpensive
D. In-line hardware keyloggers don't require physical access
Answer: B (LEAVE A REPLY)

NEW QUESTION: 58
Scenario: Your company has many encrypted telecommunications links for their world-wide operations.
Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
How can you reduce the administrative burden of distributing symmetric keys for your employer?
A. Symmetrically encrypt the key and then use asymmetric encryption to unencrypt it
B. Use a self-generated key on both ends to eliminate the need for distribution
C. Use certificate authority to distribute private keys
D. Use asymmetric encryption for the automated distribution of the symmetric key

Answer: D (LEAVE A REPLY)

NEW QUESTION: 59
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 NPV of the project is negative
B. The ROI is lower than 10 months
C. The Net Present Value (NPV) of the project is positive
D. The Return on Investment (ROI) is larger than 10 months
Answer: (SHOW ANSWER)

NEW QUESTION: 60
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 (LEAVE A REPLY)
Reference:
https://www.teamgantt.com/blog/triple-constraint-project-management#:~:text=Each%20side%20or%20point%2

NEW QUESTION: 61
Which of the following BEST describes an international standard framework that is based on the security model Information Technology-Code of Practice for Information Security Management?
A. International Organization for Standardization 27001
B. Request For Comment 2196
C. National Institute of Standards and Technology Special Publication SP 800-26
D. National Institute of Standards and Technology Special Publication SP 800-12
Answer: (SHOW ANSWER)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 62
You have implemented the new controls. What is the next step?
A. Monitor the effectiveness of the controls
B. Document the process for the stakeholders
C. Update the audit findings report
D. Perform a risk assessment
Answer: A (LEAVE A REPLY)

NEW QUESTION: 63
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 or information security strategic planning
B. 1) Cybersecurity or information security strategic planning, 2) Enterprise strategic planning, 3) Information technology strategic planning
C. 1) Enterprise strategic planning, 2) Cybersecurity or information security strategic planning, 3) Information technology strategic planning
D. 1) Enterprise strategic planning, 2) Information technology strategic planning, 3) Cybersecurity or information security strategic planning
Answer: C (LEAVE A REPLY)

NEW QUESTION: 64
Risk is defined as:
A. Advisory plus capability plus vulnerability
B. Threat times vulnerability divided by control
C. Quantitative plus qualitative impact
D. Asset loss times likelihood of event
Answer: (SHOW ANSWER)

NEW QUESTION: 65
The ability to demand the implementation and management of security controls on third parties providing services to an organization is
A. Disaster recovery
B. Compliance management
C. Security Governance
D. Vendor management
Answer: D (LEAVE A REPLY)

NEW QUESTION: 66
Risk that remains after risk mitigation is known as
A. Accepted risk

B. Persistent risk
C. Residual risk
D. Non-tolerated risk
Answer: C (LEAVE A REPLY)

NEW QUESTION: 67
An organization has a stated requirement to block certain traffic on networks. The implementation of controls will disrupt a manufacturing process and cause unacceptable delays, resulting in sever revenue disruptions.
Which of the following is MOST likely to be responsible for accepting the risk until mitigating controls can be implemented?
A. The business owner
B. The CISO
C. Audit and Compliance
D. The CFO
Answer: A (LEAVE A REPLY)

NEW QUESTION: 68
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 regulatory requirements
B. Verify capacity constraints
C. Verify the scope of the project
D. Verify technical resources
Answer: C (LEAVE A REPLY)

NEW QUESTION: 69
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, Internal Audit, Budget Authority
D. Technical Staff, Budget Authority, Management
Answer: (SHOW ANSWER)

NEW QUESTION: 70
Which of the following international standards can be BEST used to define a Risk Management process in an organization?

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

NEW QUESTION: 71
An information security department is required to remediate system vulnerabilities when they are discovered.
Please select the three primary remediation methods that can be used on an affected system.
A. Software removal, install software patch, maintain system
B. Discover software, Remove affected software, Apply software patch
C. Install software patch, Operate system, Maintain system
D. Install software patch, configuration adjustment, Software Removal
Answer: D (LEAVE A REPLY)

NEW QUESTION: 72
Assigning the role and responsibility of Information Assurance to a dedicated and independent security group is an example of:
A. Detective Controls
B. Organizational Controls
C. Proactive Controls
D. Preemptive Controls
Answer: B (LEAVE A REPLY)

NEW QUESTION: 73
The process of identifying and classifying assets is typically included in the
A. Threat analysis process
B. Business Impact Analysis
C. Asset configuration management process
D. Disaster Recovery plan
Answer: C (LEAVE A REPLY)

NEW QUESTION: 74
Credit card information, medical data, and government records are all examples of:
A. Bodily Information
B. Communications Information
C. Confidential/Protected Information
D. Territorial Information
Answer: C (LEAVE A REPLY)

NEW QUESTION: 75
A security professional has been promoted to be the CISO of an organization. The first task is to create a security policy for this organization. The CISO creates and publishes the security policy. This policy however, is ignored and not enforced consistently. Which of the following is the MOST likely reason for the policy shortcomings?
A. Lack of a formal risk management policy
B. Lack of a formal security awareness program
C. Lack of formal definition of roles and responsibilities
D. Lack of a formal security policy governance process
Answer: (SHOW ANSWER)

NEW QUESTION: 76
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. Define formal roles and responsibilities for Information Security
B. Contract a third party to perform a security risk assessment
C. Define formal roles and responsibilities for Internal audit functions
D. Create an executive security steering committee
Answer: A (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF**
Special Discount: Freepdfdumps)

NEW QUESTION: 77
Which of the following is a symmetric encryption algorithm?
A. RSA
B. ECC
C. 3DES
D. MD5
Answer: C (LEAVE A REPLY)

NEW QUESTION: 78
The PRIMARY objective for information security program development should be:
A. Establishing strategic alignment with business continuity requirements
B. Establishing incident response programs.
C. Reducing the impact of the risk to the business.
D. Identifying and implementing the best security solutions.
Answer: C (LEAVE A REPLY)

NEW QUESTION: 79
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. IT security centric agenda
B. Lack of risk management process
C. Lack of sponsorship from executive management
D. Compliance centric agenda
Answer: A (LEAVE A REPLY)

NEW QUESTION: 80
One of the MAIN goals of a Business Continuity Plan is to
A. Allow all technical first-responders to understand their roles in the event of a disaster
B. Ensure all infrastructure and applications are available in the event of a disaster
C. Assign responsibilities to the technical teams responsible for the recovery of all data.
D. Provide step by step plans to recover business processes in the event of a disaster
Answer: D (LEAVE A REPLY)

NEW QUESTION: 81
Which of the following can the company implement in order to avoid this type of security issue in the future?
A. Network based intrusion detection systems
B. A risk management process
C. A audit management process
D. A security training program for developers
Answer: (SHOW ANSWER)

NEW QUESTION: 82

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

A. Penetration testers

B. Internal Audit

C. External Audit

D. Forensic experts

Answer: C (LEAVE A REPLY)

NEW QUESTION: 83

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 has not implemented a security awareness program

C. The CISO reports to the IT organization

D. The CISO has not implemented a policy management framework

Answer: (SHOW ANSWER)

NEW QUESTION: 84

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 trial versions of commercially available security tools and deploy on your production network

B. Download open source security tools and deploy them on your production network

C. Download security tools from a trusted source and deploy to production network

D. Download open source security tools from a trusted site, test, and then deploy on production network

Answer: D (LEAVE A REPLY)

NEW QUESTION: 85

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 incident management team prepares to handle an attack

D. How the firewall and other security devices are configured to prevent attacks
Answer: (SHOW ANSWER)

NEW QUESTION: 86
Which International Organization for Standardization (ISO) below BEST describes the performance of risk management, and includes a five-stage risk management methodology.
A. ISO 27002
B. ISO 27004
C. ISO 27005
D. ISO 27001
Answer: C (LEAVE A REPLY)

NEW QUESTION: 87
Which of the following is a primary method of applying consistent configurations to IT systems?
A. Templates
B. Administration
C. Patching
D. Audits
Answer: C (LEAVE A REPLY)

NEW QUESTION: 88
What is the definition of Risk in Information Security?
A. Risk = Financial Impact x Probability
B. Risk = Probability x Impact
C. Risk = Impact x Threat
D. Risk = Threat x Probability
Answer: B (LEAVE A REPLY)

NEW QUESTION: 89
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. Setup a mock video camera next to the special card reader adjacent to the secure door

D. Educate and enforce physical security policies of the company to all the employees on a regular basis
Answer: D (LEAVE A REPLY)

NEW QUESTION: 90
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. Technical control
B. Management control
C. Procedural control
D. Administrative control
Answer: B (LEAVE A REPLY)

NEW QUESTION: 91
Which of the following is the MOST important component of any change management process?
A. Outage planning
B. Back-out procedures
C. Management approval
D. Scheduling
Answer: C (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 92
Annual Loss Expectancy is derived from the function of which two factors?
A. Single Loss Expectancy and Exposure Factor
B. Annual Rate of Occurrence and Single Loss Expectancy
C. Annual Rate of Occurrence and Asset Value
D. Safeguard Value and Annual Rate of Occurrence
Answer: (SHOW ANSWER)

NEW QUESTION: 93

When selecting a security solution with reoccurring maintenance costs after the first year (choose the BEST answer):
A. The CISO should cut other essential programs to ensure the new solution's continued use
B. Defer selection until the market improves and cash flow is positive
C. Implement the solution and ask for the increased operating cost budget when it is time
D. Communicate future operating costs to the CIO/CFO and seek commitment from them to ensure the new solution's continued use
Answer: D (LEAVE A REPLY)

NEW QUESTION: 94
How often should the Statements of Standards for Attestation Engagements-16 (SSAE16)/International Standard on Assurance Engagements 3402 (ISAE3402) report of your vendors be reviewed?
A. Bi-annually
B. Annually
C. Semi-annually
D. Quarterly
Answer: (SHOW ANSWER)

NEW QUESTION: 95
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. Scanning for viruses
B. Controlled spear phishing campaigns
C. Password changes
D. Baselining of computer systems
Answer: (SHOW ANSWER)

NEW QUESTION: 96
Which of the following information would MOST likely be reported at the board-level within an organization?
A. The capabilities of a security program in terms of staffing support
B. Significant risks and security incidents that have been discovered since the last assembly of the membership
C. System scanning trends and results as they pertain to insider and external threat sources
D. The numbers and types of cyberattacks experienced by the organization since the last assembly of the membership

Answer: B (LEAVE A REPLY)

NEW QUESTION: 97
The MOST common method to get an unbiased measurement of the effectiveness of an Information Security Management System (ISMS) is to
A. assign the responsibility to the team responsible for the management of the controls.
B. perform an independent audit of the security controls.
C. assign the responsibility to the information security team.
D. create operational reports on the effectiveness of the controls.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 98
What is the BEST way to achieve on-going compliance monitoring in an organization?
A. Outsource compliance to a 3rd party vendor and let them manage the program.
B. Have Compliance and Information Security partner to correct issues as they arise.
C. Have Compliance direct Information Security to fix issues after the auditors report.
D. Only check compliance right before the auditors are scheduled to arrive onsite.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 99
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 (LEAVE A REPLY)

NEW QUESTION: 100
What is the primary reason for performing vendor management?
A. To document the relationship between the company and the vendor
B. To establish a vendor selection process
C. To define the partnership for long-term success
D. To understand the risk coverage that are being mitigated by the vendor
Answer: D (LEAVE A REPLY)

NEW QUESTION: 101
Acceptable levels of information security risk tolerance in an organization should be determined by?
A. CEO and board of director
B. Corporate compliance committee

C. CISO with reference to the company goals
D. Corporate legal counsel
Answer: A (LEAVE A REPLY)

NEW QUESTION: 102
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.
What action should you take FIRST?
A. Destroy the repository of stolen data
B. Contract with a credit reporting company for paid monitoring services for affected customers
C. Contact your local law enforcement agency
D. Consult with other C-Level executives to develop an action plan
Answer: D (LEAVE A REPLY)

NEW QUESTION: 103
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 will ultimately use the system.
D. That has budget authority.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 104
As a new CISO at a large healthcare company you are told that everyone has to badge in to get in the building.
Below your office window you notice a door that is normally propped open during the day for groups of people to take breaks outside. Upon looking closer you see there is no badge reader. What should you do?
A. Have a risk assessment performed.
B. Nothing, this falls outside your area of influence.
C. Post a guard at the door to maintain physical security
D. Close and chain the door shut and send a company-wide memo banning the practice.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 105
When managing the critical path of an IT security project, which of the following is MOST important?
A. Knowing the threats to the organization.
B. Knowing who all the stakeholders are.
C. Knowing the people on the data center team.
D. Knowing the milestones and timelines of deliverables.
Answer: D (LEAVE A REPLY)

NEW QUESTION: 106
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. IDS, syslog, router, switches
C. Firewall, exchange, web server, intrusion detection system (IDS)
D. Firewall, anti-virus console, IDS, syslog
Answer: D (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 107
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: (SHOW ANSWER)
Reference: https://searchsecurity.techtarget.com/definition/intrusion-prevention

NEW QUESTION: 108
The effectiveness of an audit is measured by?
A. The number of security controls the company has in use
B. How it exposes the risk tolerance of the company
C. How the recommendations directly support the goals of the company
D. The number of actionable items in the recommendations
Answer: C (LEAVE A REPLY)

NEW QUESTION: 109
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: (SHOW ANSWER)

NEW QUESTION: 110
Scenario: Your company has many encrypted telecommunications links for their world-wide operations.
Physically distributing symmetric keys to all locations has proven to be administratively burdensome, but symmetric keys are preferred to other alternatives.
Symmetric encryption in general is preferable to asymmetric encryption when:
A. The speed of the encryption / deciphering process is essential
B. The number of unique communication links is large
C. The volume of data being transmitted is small
D. The distance to the end node is farthest away
Answer: A (LEAVE A REPLY)

NEW QUESTION: 111
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. Compliance with local government privacy laws
B. International encryption restrictions
C. Adherence to local data breach notification laws
D. Compliance to Payment Card Industry (PCI) data security standards
Answer: D (LEAVE A REPLY)

NEW QUESTION: 112
The process to evaluate the technical and non-technical security controls of an IT system to validate that a given design and implementation meet a specific set of security requirements is called
A. Security system analysis
B. Security accreditation
C. Alignment with business practices and goals.
D. Security certification
Answer: D (LEAVE A REPLY)

NEW QUESTION: 113
In order for a CISO to have true situational awareness there is a need to deploy technology that can give a real-time view of security events across the enterprise. Which tool selection represents the BEST choice to achieve situational awareness?
A. SIEM, IDS, firewall, VMS
B. Vmware, router, switch, firewall, syslog, vulnerability management system (VMS)
C. Security Incident Event Management (SIEM), IDS, router, syslog
D. Intrusion Detection System (IDS), firewall, switch, syslog
Answer: A (LEAVE A REPLY)

NEW QUESTION: 114
Which of the following is the MOST important reason to measure the effectiveness of an Information Security Management System (ISMS)?
A. Meet regulatory compliance requirements
B. Better understand strengths and weaknesses of the program
C. Better understand the threats and vulnerabilities affecting the environment
D. Meet legal requirements
Answer: (SHOW ANSWER)

NEW QUESTION: 115
With respect to the audit management process, management response serves what function?
A. adding controls to ensure that proper oversight is achieved by management
B. determining whether or not resources will be allocated to remediate a finding

C. revealing the "root cause" of the process failure and mitigating for all internal and external units
D. placing underperforming units on notice for failing to meet standards
Answer: B (LEAVE A REPLY)

NEW QUESTION: 116
You are the Chief Information Security Officer of a large, multinational bank and you suspect there is a flaw in a two factor authentication token management process. Which of the following represents your BEST course of action?
A. Validate that security awareness program content includes information about the potential vulnerability
B. Conduct a thorough risk assessment against the current implementation to determine system functions
C. Send a report to executive peers and business unit owners detailing your suspicions
D. Determine program ownership to implement compensating controls
Answer: (SHOW ANSWER)

NEW QUESTION: 117
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 establishes a framework to protect confidential information
D. it defines a process to meet compliance requirements
Answer: A (LEAVE A REPLY)

NEW QUESTION: 118
Which of the following will be MOST helpful for getting an Information Security project that is behind schedule back on schedule?
A. Involve internal audit
B. Upper management support
C. More training of staff members
D. More frequent project milestone meetings
Answer: B (LEAVE A REPLY)

NEW QUESTION: 119
Which of the following activities is the MAIN purpose of the risk assessment process?
A. Creating an inventory of information assets
B. Classifying and organizing information assets into meaningful groups
C. Calculating the risks to which assets are exposed in their current setting
D. Assigning value to each information asset
Answer: C (LEAVE A REPLY)

NEW QUESTION: 120
The formal certification and accreditation process has four primary steps, what are they?
A. Evaluating, purchasing, testing, authorizing
B. Discovery, testing, authorizing, certifying
C. Auditing, documenting, verifying, certifying
D. Evaluating, describing, testing and authorizing
Answer: D (LEAVE A REPLY)

NEW QUESTION: 121
Regulatory requirements typically force organizations to implement
A. Mandatory controls
B. Financial controls
C. Optional controls
D. Discretionary controls
Answer: A (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 122
Many times a CISO may have to speak to the Board of Directors (BOD) about their cyber security posture.
What would be the BEST choice of security metrics to present to the BOD?
A. All vulnerabilities found on servers and desktops
B. Only critical and high vulnerabilities on servers and desktops
C. Only critical and high vulnerabilities that impact important production servers
D. All vulnerabilities that impact important production servers
Answer: C (LEAVE A REPLY)

NEW QUESTION: 123
Which of the following is a critical operational component of an Incident Response Program (IRP)?
A. Daily monitoring of vulnerability advisories relating to your organization's deployed technologies.

B. Annual review of program charters, policies, procedures and organizational agreements.
C. Monthly program tests to ensure resource allocation is sufficient for supporting the needs of the organization
D. Weekly program budget reviews to ensure the percentage of program funding remains constant.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 124
Which of the following strategies provides the BEST response to a ransomware attack?
A. Daily incremental backup
B. Daily differential backup
C. Daily full backup
D. Real-time off-site replication
Answer: A (LEAVE A REPLY)

NEW QUESTION: 125
An organization information security policy serves to
A. establish acceptable systems and user behavior
B. establish budgetary input in order to meet compliance requirements
C. define relationships with external law enforcement agencies
D. define security configurations for systems
Answer: A (LEAVE A REPLY)

NEW QUESTION: 126
As the CISO, you have been tasked with the execution of the company's key management program. You MUST ensure the integrity of encryption keys at the point of generation. Which principal of encryption key control will ensure no single individual can constitute or re-constitute a key?
A. Dual Control
B. Separation of Duties
C. Split Knowledge
D. Least Privilege
Answer: A (LEAVE A REPLY)
Reference: https://info.townsendsecurity.com/bid/23881/PCI-DSS-2-0-and-Encryption-Key-Management

NEW QUESTION: 127
Which of the following functions evaluates patches used to close software vulnerabilities of new systems to assure compliance with policy when implementing an information security program?

A. Planning
B. Incident response
C. System testing
D. Risk assessment
Answer: C (LEAVE A REPLY)

NEW QUESTION: 128
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 of unplanned outages
C. Number and length of planned outages
D. Number of change orders processed
Answer: B (LEAVE A REPLY)

NEW QUESTION: 129
Which of the following is the PRIMARY purpose of International Organization for Standardization (ISO)
27001?
A. Implementation of business-enabling information security
B. Use within an organization to ensure compliance with laws and regulations
C. Use within an organization to formulate security requirements and objectives
D. To enable organizations that adopt it to obtain certifications
Answer: (SHOW ANSWER)

NEW QUESTION: 130
The process for identifying, collecting, and producing digital information in support of legal proceedings is called
A. electronic discovery.
B. evidence tampering.
C. chain of custody.
D. electronic review.
Answer: A (LEAVE A REPLY)

NEW QUESTION: 131
Which of the following represents the best method of ensuring business unit alignment with security program requirements?
A. Demonstrate executive support with written mandates for security policy adherence

B. Perform increased audits of security processes and procedures
C. Provide clear communication of security requirements throughout the organization
D. Create collaborative risk management approaches within the organization
Answer: D (LEAVE A REPLY)

NEW QUESTION: 132
A CISO has implemented a risk management capability within the security portfolio. Which of the following terms best describes this functionality?
A. Cost center
B. Portfolio
C. Service
D. Program
Answer: D (LEAVE A REPLY)

NEW QUESTION: 133
The success of the Chief Information Security Officer is MOST dependent upon:
A. raising awareness of security issues with end users
B. following the recommendations of consultants and contractors
C. development of relationships with organization executives
D. favorable audit findings
Answer: (SHOW ANSWER)

NEW QUESTION: 134
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 variety of technologies deployed in the infrastructure.
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 need to develop a more unified incident response capability.
D. When it results in an overall lower cost of operating the security program.
Answer: B (LEAVE A REPLY)

NEW QUESTION: 135
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 (LEAVE A REPLY)
Reference: https://searchnetworking.techtarget.com/definition/Snort

NEW QUESTION: 136
Which business stakeholder is accountable for the integrity of a new information system?
A. Project manager
B. Compliance Officer
C. CISO
D. Board of directors
Answer: C (LEAVE A REPLY)

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)

NEW QUESTION: 137
Which of the following is MOST important when tuning an Intrusion Detection System (IDS)?
A. Type of authentication
B. Log retention
C. Trusted and untrusted networks
D. Storage encryption
Answer: C (LEAVE A REPLY)

NEW QUESTION: 138
The primary purpose of a risk register is to:
A. Maintain a log of discovered risks
B. Track individual risk assessments
C. Develop plans for mitigating identified risks
D. Coordinate the timing of scheduled risk assessments

Answer: A (LEAVE A REPLY)
Reference: https://sitemate.com/us/resources/articles/safety/purpose-of-a-risk-register/

NEW QUESTION: 139
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 forecast usage and cost per software licensing
C. To communicate risk and forecast resource needs
D. To understand the attack vectors and attack sources
Answer: C (LEAVE A REPLY)

NEW QUESTION: 140
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 (LEAVE A REPLY)
Reference: https://www.resolver.com/resource/bcdr-metrics-that-matter/

Valid 512-50 Dumps shared by Actual4test.com for Helping Passing 512-50 Exam! Actual4test.com now offer the **newest 512-50 exam dumps**, the Actual4test.com 512-50 exam **questions have been updated** and **answers have been corrected** get the **newest** Actual4test.com 512-50 dumps with Test Engine here: https://www.actual4test.com/512-50_examcollection.html (**402** Q&As Dumps, **30%OFF** **Special Discount: Freepdfdumps**)