

ISC.CISSP-ISSMP.v2026-10-01.q228

Exam Code:	CISSP-ISSMP
Exam Name:	CISSP-ISSMP - Information Systems Security Management Professional
Certification Provider:	ISC
Free Question Number:	228
Version:	v2026-10-01
# of views:	108
# of Questions views:	2507
https://www.dumpsfiles.com/files/ISC/CISSP-ISSMP/ISC.CISSP-ISSMP.v2026-10-01.q228	

NEW QUESTION: 1

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution.

Which of the following data should be recorded in this documentation? Each correct answer represents a complete solution. Choose all that apply.

- A. Location of each incident
- B. Names of the victims
- C. Nature of harassment
- D. Date and time of incident

Answer: A,B,D (LEAVE A REPLY)

NEW QUESTION: 2

Which of the following BEST describes "attack surface reduction" as a strategic security objective?

- A. Increasing the number of exposed services to improve visibility
- B. Minimizing the number of potential entry points (services, ports, accounts, code) available to an attacker
- C. Attack surface reduction applies only to network firewalls
- D. It is achieved solely through employee training

Answer: B (LEAVE A REPLY)

Reducing unnecessary services, open ports, excess privileges, and unused code/features shrinks the number of ways an attacker could potentially gain access, a core proactive risk reduction strategy.

NEW QUESTION: 3

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Assessing the impact of potential threats
- B. Identifying the accused

C. Identifying the risk

D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Answer: A,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 4

You are the project manager of the NGQQ Project for your company. To help you communicate project status to your stakeholders, you are going to create a stakeholder register. All of the following information should be included in the stakeholder register except for which one?

A. Identification information for each stakeholder

B. Assessment information of the stakeholders' major requirements, expectations, and potential influence

C. Stakeholder classification of their role in the project

D. Stakeholder management strategy

Answer: D ([LEAVE A REPLY](#))

The stakeholder management strategy is generally not included in the stakeholder registry because it may contain sensitive information that should not be shared with project team members or certain other individuals that could see the stakeholder register. The stakeholder register is a project management document that contains a list of the stakeholders associated with the project. It assesses how they are involved in the project and identifies what role they play in the organization. The information in this document can be very perceptive and is meant for limited exchange only. It also contains relevant information about the stakeholders, such as their requirements, expectations, and influence on the project. Answer option A is incorrect.

Stakeholder identification should be included in the stakeholder register.

Answer option B is incorrect. Assessment information should be included in the stakeholder register. Answer option C is incorrect.

Stakeholder classification should be included in the stakeholder register.

Reference: "Project Management Body of Knowledge (PMBOK Guide), Fourth Edition"

NEW QUESTION: 5

Which of the following BEST describes the concept of "security debt," analogous to "technical debt"?

A. Security debt refers only to unpaid vendor invoices

B. Accumulated deferred security work (unpatched systems, unaddressed findings, expired exceptions) that increases organizational risk exposure over time if not addressed

C. Security debt is a formal accounting term with no risk management relevance

D. Security debt automatically resolves itself over time without intervention

Answer: B ([LEAVE A REPLY](#))

Similar to technical debt, security debt accumulates when remediation, patching, or control improvements are deferred; left unaddressed, this backlog compounds risk exposure and often becomes more costly to resolve later.

NEW QUESTION: 6

Which of the following contract types is described in the statement below? "This contract type provides no incentive for the contractor to control costs and hence is rarely utilized."

A. Cost Plus Fixed Fee

B. Cost Plus Percentage of Cost

C. Cost Plus Incentive Fee

D. Cost Plus Award Fee

Answer: B ([LEAVE A REPLY](#))

Cost Plus Percentage of Cost contracts pay a fee that rises as the contractors cost rise. Because this contract type provides no incentive for the contractor to control costs, it is rarely utilized. The U.S. Federal Acquisition Regulations specifically prohibit the use of this type for U.S. Federal Government contracting.

NEW QUESTION: 7

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

A. No

B. Yes

Answer: B ([LEAVE A REPLY](#))

Sarah is guilty under copyright laws because pleading ignorance of copyright infringement is not an excuse.

What is copyright?

A copyright is a form of intellectual property, which secures to its holder the exclusive right to produce copies of his or her works of original expression, such as a literary work, movie, musical work or sound recording, painting, photograph, computer program, or industrial design, for a defined, yet extendable, period of time. It does not cover ideas or facts. Copyright laws protect intellectual property from misuse by other individuals.

Reference: "<http://en.wikipedia.org/wiki/Copyright>"

NEW QUESTION: 8

Which of the following statements about Due Care policy is true?

A. It identifies the level of confidentiality of information.

B. It provides information about new viruses.

C. It is a method used to authenticate users on a network.

D. It is a method for securing database servers.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 9

Which of the following BEST describes why "operational threat intelligence" is particularly useful during active incident response?

A. It focuses only on long-term geopolitical trends

B. It provides specific, timely details about an ongoing campaign or specific threat actor's current activity relevant to the incident at hand

C. It is identical to strategic intelligence

D. It is irrelevant during active incidents

Answer: B ([LEAVE A REPLY](#))

Operational intelligence provides context-specific details about a particular campaign/actor (infrastructure, targeting, objectives) that responders can use directly to inform containment and eradication decisions during an active incident.

NEW QUESTION: 10

Rachael is the project manager for a large project in her organization. A new change request has been proposed that will affect several areas of the project. One area of the project change impact is on work that a vendor has already completed. The vendor is refusing to make the changes as they've already completed the project work they were contracted to do. What can Rachael do in this instance?

- A. Refer to the contract agreement for direction.
- B. Fire the vendor for failing to complete the contractual obligation.
- C. Withhold the vendor's payments for the work they've completed.
- D. Threaten to sue the vendor if they don't complete the work.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 11

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat- source and to identify potential failures in the IT system protection schemes?

- A. Penetration testing
- B. Security Test and Evaluation (ST&E)
- C. On-site interviews
- D. Automated vulnerability scanning tool

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 12

Which of the following protocols is used with a tunneling protocol to provide security?

- A. IPX/SPX
- B. EAP
- C. FTP
- D. IPSec

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 13

You work as a Senior Marketing Manger for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident.

Which of the following steps of an incident handling process was performed by the incident response team?

- A. Containment
- B. Eradication
- C. Preparation
- D. Identification

Answer: D ([LEAVE A REPLY](#))

According to the question, incident response team announced that this was a controlled event not an incident. Incident response team performed the identification step to rectify the incident.

Identification is the first post-attack step in Incident handling process. In this phase of the incident handling process, the Incident Handler determines whether the incident exists or not. An incident is described as an event in a system or network that poses threat to the environment.

Identification of an incident becomes more difficult with the increase in the complexity of the attack. The Incident Handler should gather all facts and make decisions on the basis of those facts. Incident Handler needs to identify the following characteristics of an attack before it can be properly processed.

NEW QUESTION: 14

You work as a security manager for SoftTech Inc. You along with your team are doing the disaster recovery for your project. Which of the following steps are performed by you for secure recovery based on the extent of the disaster and the organization's recovery ability? Each correct answer represents a part of the solution. Choose three.

- A.** Recover to an alternate site for critical functions
- B.** Restore full system at an alternate operating site
- C.** Restore full system after a catastrophic loss
- D.** Recover at the primary operating site

Answer: ([SHOW ANSWER](#))

The steps performed for secure recovery in disasters is based on the extent of the disaster and the organization's recovery ability. The steps performed for secure recovery are as follows .

Recover at the primary operating site.

Recover to an alternate site for critical functions.

Restore full system after a catastrophic loss.

Answer option B is incorrect. This is not a valid answer for this Question.

Reference:

CISM Review Manual 2010, Contents. "Incident Management and Response"

NEW QUESTION: 15

You are a project manager of a large construction project. Within the project you are working with several vendors to complete different phases of the construction. Your client has asked that you arrange for some of the materials a vendor is to install next week in the project to be changed.

According to the change management plan what subsystem will need to manage this change request?

- A.** Cost
- B.** Resources
- C.** Contract
- D.** Schedule

Answer: **C** ([LEAVE A REPLY](#))

Because the vendor is completing the work the change request will need to move through the contract change control system. There are four change control systems in project management:

scope, cost, schedule, and contract. If the scope change control were a choice, it would be a valid answer too.

NEW QUESTION: 16

Which of the following relies on a physical characteristic of the user to verify his identity?

- A. Social Engineering
- B. Kerberos v5
- C. Biometrics
- D. CHAP

Answer: C ([LEAVE A REPLY](#))

Biometrics is a method of authentication that uses physical characteristics, such as fingerprints, scars, retinal patterns, and other forms of biophysical qualities to identify a user. Nowadays, the usage of biometric devices such as hand scanners and retinal scanners is becoming more common in the business environment.

Answer option B is incorrect. Kerberos v5 is an authentication method used by Windows operating systems to authenticate users and network services. Windows 2000/2003 and XP clients and servers use Kerberos v5 as the default authentication method. Kerberos has replaced the NT LAN Manager (NTLM) authentication method, which was less secure. Kerberos uses mutual authentication to verify both the identity of the user and network services. The Kerberos authentication process is transparent to the users.

Note: Kerberos v5 is not supported on Windows XP Home clients or on any clients that are not members of an Active Directory domain.

Answer option A is incorrect. Social engineering is the art of convincing people and making them disclose useful information such as account names and passwords. This information is further exploited by hackers to gain access to a user's computer or network. This method involves mental ability of the people to trick someone rather than their technical skills. A user should always distrust people who ask him for his account name or password, computer name, IP address, employee ID, or other information that can be misused.

Answer option D is incorrect. Challenge Handshake Authentication Protocol (CHAP) is an authentication protocol that uses a secure form of encrypted authentication. Using CHAP, network dial-up connections are able to securely connect to almost all PPP servers.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 17

Which of the following are the goals of risk management? Each correct answer represents a complete solution. Choose three.

- A. Assessing the impact of potential threats
- B. Identifying the accused
- C. Finding an economic balance between the impact of the risk and the cost of the countermeasure
- D. Identifying the risk

Answer: A,C,D ([LEAVE A REPLY](#))

There are three goals of risk management as follows:

Identifying the risk

Assessing the impact of potential threats

Finding an economic balance between the impact of the risk and the cost of the countermeasure Answer option B is incorrect. Identifying the accused does not come under the scope of risk management.

Reference: "http://en.wikipedia.org/wiki/Risk_management"

NEW QUESTION: 18

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

- A. Integrity
- B. Availability
- C. Encryption
- D. Confidentiality

Answer: [\(SHOW ANSWER\)](#)

NEW QUESTION: 19

Which of the following is the BEST justification for implementing "network segmentation" between IT and OT (Operational Technology) environments in a manufacturing organization?

- A. Segmentation is unnecessary since OT systems are inherently secure
- B. Segmentation limits an attacker's ability to move laterally from a compromised IT network into safety-critical OT systems, reducing potential physical/safety impact
- C. IT and OT systems should always share the same network for efficiency
- D. Segmentation eliminates the need for OT-specific security controls

Answer: B [\(LEAVE A REPLY\)](#)

OT environments often control physical processes with safety implications; segmenting them from the (typically more exposed) IT network limits the blast radius of an IT compromise and reduces risk of attackers reaching safety-critical systems.

NEW QUESTION: 20

Which of the following BEST describes why "single sign-on (SSO)" implementations require careful risk consideration despite usability benefits?

- A. SSO has no security risk implications
- B. While SSO improves usability, a compromised SSO credential can grant broader access across multiple systems, increasing the impact of account compromise
- C. SSO always reduces risk with no tradeoffs
- D. SSO is relevant only to physical access control

Answer: B [\(LEAVE A REPLY\)](#)

SSO centralizes authentication, improving user experience and reducing password fatigue, but also concentrates risk - a single compromised credential can expose multiple connected systems, making strong authentication (e.g., MFA) especially critical.

NEW QUESTION: 21

Which of the following is the PRIMARY reason for maintaining an updated asset inventory as part of a security program?

- A. To simplify procurement paperwork
- B. To ensure all assets requiring protection are identified, since unknown assets cannot be adequately secured
- C. To track employee attendance
- D. To calculate depreciation for tax purposes only

Answer: B [\(LEAVE A REPLY\)](#)

You cannot protect what you don't know exists - asset inventory is foundational to risk assessment, vulnerability management, and incident response scoping.

NEW QUESTION: 22

You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:

Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

- A. \$41,750
- B. \$142,000
- C. \$232,000
- D. \$23,750

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 23

Which of the following steps are generally followed in computer forensic examinations? Each correct answer represents a complete solution. Choose three.

- A. Acquire
- B. Analyze
- C. Authenticate
- D. Encrypt

Answer: A,B,C ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 24

Which of the following is the BEST approach when a critical vulnerability is identified in a legacy system that cannot be patched due to vendor end-of-life status?

- A. Ignore the vulnerability since patching isn't possible
- B. Implement compensating controls (e.g., network segmentation, enhanced monitoring) and develop a risk-based remediation/replacement plan
- C. Immediately decommission the system without business consultation
- D. Accept the risk without documentation

Answer: ([SHOW ANSWER](#))

When patching isn't feasible, compensating controls reduce exposure while a longer-term plan (replacement, upgrade, or formal risk acceptance) is developed - a balanced, documented risk management response.

NEW QUESTION: 25

Which of the following contract types is described in the statement below? "This contract type provides no incentive for the contractor to control costs and hence is rarely utilized."

- A. Cost Plus Percentage of Cost
- B. Cost Plus Award Fee
- C. Cost Plus Fixed Fee
- D. Cost Plus Incentive Fee

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 26

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network.

John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

- A. Operational audit
- B. Dependent audit
- C. Non-operational audit
- D. Independent audit

Answer: (SHOW ANSWER)

An independent audit is an audit that is usually conducted by external or outside resources. It is the process of reviewing detailed audit logs for the following purposes:

To examine the system activities and access logs

To assess the adequacy of system methods

To assess the adequacy of system controls

To examine compliance with established enterprise network system policies To examine compliance with established enterprise network system procedures To examine effectiveness of enabling, support, and core processes Answer option B is incorrect. It is not a valid type of security audit.

Answer option A is incorrect. It is done to examine the operational and ongoing activities within a network.

Answer option C is incorrect. It is not a valid type of security audit.

Reference: Guide to Tactical Perimeter Defense, Contents: "Network Auditing Concepts"

NEW QUESTION: 27

Which of the following BEST describes why "geographic diversity" between primary and backup/DR sites is an important planning consideration?

- A. Geographic diversity is unnecessary if both sites have strong physical security
- B. Sites located too close together may be simultaneously affected by the same regional disaster (e.g., earthquake, hurricane, power grid failure)
- C. Geographic diversity only matters for international organizations
- D. Geographic diversity guarantees zero downtime during any disaster

Answer: B ([LEAVE A REPLY](#))

If primary and backup sites share the same regional risk exposure (e.g., same power grid, same flood zone), a single event could disable both simultaneously; sufficient geographic separation reduces this correlated risk.

NEW QUESTION: 28

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Request for service, initial analysis, data collection, data reporting, data analysis
- B. Initial analysis, request for service, data collection, data analysis, data reporting
- C. Request for service, initial analysis, data collection, data analysis, data reporting
- D. Initial analysis, request for service, data collection, data reporting, data analysis

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 29

In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

- A. Discretionary Access Control
- B. Role-Based Access Control
- C. Task-based Access Control
- D. Mandatory Access Control

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 30

DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997.

What phases are identified by DIACAP?

Each correct answer represents a complete solution. Choose all that apply.

- A. System Definition
- B. Accreditation
- C. Verification
- D. Re-Accreditation
- E. Validation
- F. Identification

Answer: A,C,D,E ([LEAVE A REPLY](#))

The Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) is a process defined by the United States Department of Defense (DoD) for managing risk. DIACAP replaced the former process, known as DITSCAP (Department of Defense Information Technology Security Certification and Accreditation Process), in 2006. DoD Instruction (DoDI) 8510.01 establishes a standard DoD-wide process with a set of activities, general tasks, and a management structure to certify and accredit an Automated Information System (AIS) that will maintain the Information Assurance (IA) posture of the Defense Information Infrastructure (DII) throughout the system's life cycle. DIACAP applies to the acquisition, operation, and sustainment of any DoD system that collects, stores, transmits, or processes unclassified or classified information since December 1997. It identifies four phases.

1. System Definition
2. Verification

3.Validation

4.Re-Accreditation

http://en.wikipedia.org/wiki/Department_of_Defense_Information_Technology_Security_Certification_and_Accreditation_Process

NEW QUESTION: 31

Which of the following security models dictates that subjects can only access objects through applications?

A. Biba-Clark model

B. Bell-LaPadula

C. Clark-Wilson

D. Biba model

Answer: C ([LEAVE A REPLY](#))

The Clark-Wilson security model dictates that subjects can only access objects through applications. Answer option D is incorrect. The Biba model does not let subjects write to objects at a higher integrity level.

Answer option B is incorrect. The Bell-LaPadula model has a simple security rule, which means a subject cannot read data from a higher level.

Answer option A is incorrect. There is no such model as Biba-Clark model.

Reference: "http://en.wikipedia.org/wiki/Clark-Wilson_model"

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 32

SIMULATION

Fill in the blank with the appropriate phrase. _____ is the ability to record and report on the configuration baselines associated with each configuration item at any moment of time.

Answer:

Configuration status accounting

NEW QUESTION: 33

Which of the following BEST describes why security managers should track "control effectiveness" separately from "control existence"?

A. If a control exists, it is automatically assumed to be effective

B. A control may be formally implemented (exists) but fail to operate as intended (ineffective) due to misconfiguration, gaps, or process failure

C. Control effectiveness is irrelevant once implementation is complete

D. Only technical controls require effectiveness testing

Answer: B ([LEAVE A REPLY](#))

Documented policy or a deployed tool doesn't guarantee it's functioning correctly; ongoing testing/monitoring is needed to confirm controls are actually reducing risk as designed, not just present on paper.

NEW QUESTION: 34

Which of the following refers to an information security document that is used in the United States Department of Defense (DoD) to describe and accredit networks and systems?

- A.** SSAA
- B.** FITSAF
- C.** FIPS
- D.** TCSEC

Answer: A (LEAVE A REPLY)

System Security Authorization Agreement (SSAA) is an information security document used in the United States Department of Defense (DoD) to describe and accredit networks and systems.

The SSAA is part of the Department of Defense Information Technology Security Certification and Accreditation Process, or DITSCAP.

The DoD instruction (issued in December 1997, that describes DITSCAP and provides an outline for the SSAA document is DODI 5200.40. The DITSCAP application manual (DoD 8510.1-M), published in July 2000, provides additional details.

Answer option B is incorrect. FITSAF stands for Federal Information Technology Security Assessment Framework. It is a methodology for assessing the security of information systems. It provides an approach for federal agencies. It determines how federal agencies are meeting existing policy and establish goals. The main advantage of FITSAF is that it addresses the requirements of Office of Management and Budget (OMB). It also addresses the guidelines provided by the National Institute of Standards and Technology (NIST).

Answer option D is incorrect. Trusted Computer System Evaluation Criteria (TCSEC) is a United States Government Department of Defense (DoD) standard that sets basic requirements for assessing the effectiveness of computer security controls built into a computer system. TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information. It was replaced with the development of the Common Criteria international standard originally published in 2005. The TCSEC, frequently referred to as the Orange Book, is the centerpiece of the DoD Rainbow Series publications.

NEW QUESTION: 35

Which of the following processes is used by remote users to make a secure connection to internal resources after establishing an Internet connection?

- A.** Packet filtering
- B.** Tunneling
- C.** Packet sniffing
- D.** Spoofing

Answer: B (LEAVE A REPLY)

Tunneling is a process used by remote users to make a secure connection to internal resources after establishing an Internet connection. The tunnel is created between the two ends by encapsulating the data in a mutually agreed-upon protocol for transmission.

Answer option A is incorrect. Packet filtering is a method that allows or restricts the flow of specific types of packets to provide security. It analyzes the incoming and outgoing packets and lets them pass or stops them at a network interface based on the source and destination addresses, ports, or protocols. Packet filtering provides a way to define precisely which type of IP traffic is allowed to cross the firewall of an intranet. IP packet filtering is important when users from private intranets connect to public networks, such as the Internet.

Answer option C is incorrect. Packet sniffing is a process of monitoring data packets that travel across a network. The software used for packet sniffing is known as sniffers. There are many packet- sniffing programs that are available on the Internet. Some of these are unauthorized, which can be harmful for a network's security.

Answer option D is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity. However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

NEW QUESTION: 36

You work as a Senior Marketing Manger for Umbrella Inc. You find out that some of the software applications on the systems were malfunctioning and also you were not able to access your remote desktop session. You suspected that some malicious attack was performed on the network of the company. You immediately called the incident response team to handle the situation who enquired the Network Administrator to acquire all relevant information regarding the malfunctioning. The Network Administrator informed the incident response team that he was reviewing the security of the network which caused all these problems. Incident response team announced that this was a controlled event not an incident. Which of the following steps of an incident handling process was performed by the incident response team?

- A. Preparation
- B. Identification
- C. Containment
- D. Eradication

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 37

Which of the following is the PRIMARY reason to conduct a lessons-learned session after a disaster recovery test, even if the test was "successful"?

- A. To assign blame for any delays
- B. To identify gaps and opportunities for improvement even in successful outcomes
- C. To satisfy insurance requirements only
- D. To reduce the frequency of future testing

Answer: B ([LEAVE A REPLY](#))

Even successful tests reveal opportunities for refinement (timing, communication, documentation gaps); continuous improvement is the goal regardless of outcome, not blame assignment or reduced testing.

NEW QUESTION: 38

Which of the following access control models uses a predefined set of access privileges for an object of a system?

- A. Role-Based Access Control
- B. Mandatory Access Control
- C. Discretionary Access Control
- D. Policy Access Control

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 39

Which of the following BEST describes the purpose of a Memorandum of Understanding (MOU) in the context of contingency planning?

- A. It legally binds a vendor to specific service levels
- B. It documents a general agreement of intent between parties regarding mutual aid or cooperation
- C. It replaces the need for a formal contract
- D. It guarantees financial compensation in case of disaster

Answer: ([SHOW ANSWER](#))

An MOU expresses mutual intent to cooperate (e.g., reciprocal site agreements) but is generally not as legally binding or detailed as a formal contract or SLA. Answer option A describes an SLA; C and D overstate the MOU's legal weight.

NEW QUESTION: 40

Which of the following BEST describes why "communication redundancy" (multiple channels) is built into crisis communication plans?

- A. A single communication channel is always sufficient
- B. If the primary communication channel (e.g., corporate email) is unavailable during a disruption, alternate channels ensure critical messages still reach stakeholders
- C. Communication redundancy applies only to external stakeholders, never internal staff
- D. Redundant channels increase risk of message inconsistency and should be avoided

Answer: B ([LEAVE A REPLY](#))

A disaster affecting IT infrastructure could also disable the primary communication tool itself (e.g., email server down); having backup channels (text alerts, phone trees, external notification services) ensures continuity of communication.

NEW QUESTION: 41

Which of the following are the goals of risk management? Each correct answer represents a complete solution.

Choose three.

- A. Identifying the risk
- B. Identifying the accused
- C. Assessing the impact of potential threats
- D. Finding an economic balance between the impact of the risk and the cost of the countermeasure

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 42

Which of the following access control models are used in the commercial sector? Each correct answer represents a complete solution.

Choose two.

- A. Clark-Biba model
- B. Clark-Wilson model
- C. Bell-LaPadula model
- D. Biba model

Answer: B,D ([LEAVE A REPLY](#))

The Biba and Clark-Wilson access control models are used in the commercial sector. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or

be corrupted by data from a lower level than the subject. The Clark-Wilson security model provides a foundation for specifying and analyzing an integrity policy for a computing system.

Answer option C is incorrect. The Bell-LaPadula access control model is mainly used in military systems.

Answer option A is incorrect. There is no such access control model as Clark-Biba.

Reference: "<http://en.wikipedia.org/wiki/Biba>"

NEW QUESTION: 43

Tomas is the project manager of the QWS Project and is worried that the project stakeholders will want to change the project scope frequently. His fear is based on the many open issues in the project and how the resolution of the issues may lead to additional project changes. On what document are Tomas and the stakeholders working in this scenario?

- A.** Change management plan
- B.** Risk management plan
- C.** Issue log
- D.** Communications management plan

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 44

Sarah, a CISO, wants to measure how quickly her SOC detects and responds to incidents. Which metrics should she track?

- A.** Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR)
- B.** Number of employees trained
- C.** Number of open vulnerabilities
- D.** Annual security budget

Answer: A ([LEAVE A REPLY](#))

MTTD and MTTR are standard operational metrics for evaluating detection and response efficiency. Answer options B, C, and D measure other program aspects, not response speed.

NEW QUESTION: 45

Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

- A.** Second Code of Ethics Canons
- B.** Fourth Code of Ethics Canons
- C.** First Code of Ethics Canons
- D.** Third Code of Ethics Canons

Answer: ([SHOW ANSWER](#))

The Code of Ethics Canons in (ISC)2 code of ethics are as follows. Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.

Reference: <https://www.isc2.org/ethics/default.aspx>

NEW QUESTION: 46

Which of the following BEST describes why "tabletop exercises should include realistic constraints" (e.g., limited communication, partial information) rather than idealized scenarios?

- A. Realistic constraints make exercises unnecessarily difficult and should be avoided
- B. Realistic constraints better simulate actual crisis conditions, testing the team's ability to make decisions under genuine uncertainty and pressure
- C. Idealized scenarios are always more effective for training purposes
- D. Constraints are only relevant for technical, not executive, exercises

Answer: ([SHOW ANSWER](#))

Real incidents rarely provide complete, clean information; incorporating realistic ambiguity, communication breakdowns, or incomplete data into exercises better prepares teams for the actual conditions they'll face during a genuine crisis.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 47

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Direct
- B. Circumstantial
- C. Incontrovertible
- D. Corroborating

Answer: ([SHOW ANSWER](#))

Circumstantial evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person. Answer option D is incorrect.

Corroborating evidence is evidence that tends to support a proposition that is already supported by some evidence.

Answer option C is incorrect. Incontrovertible evidence is a colloquial term for evidence introduced to prove a fact that is supposed to be so conclusive that there can be no other truth as to the matter; evidence so strong, it overpowers contrary evidence, directing a fact-finder to a specific and certain conclusion.

Answer option A is incorrect. Direct evidence is testimony proof for any evidence, which expressly or straight-forwardly proves the existence of a fact.

NEW QUESTION: 48

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

- A. Recreating and analyzing the problem
- B. Performing quality control

- C. Establishing the priorities of requests
- D. Developing the changes and corresponding tests

Answer: A,B,D ([LEAVE A REPLY](#))

NEW QUESTION: 49

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

- A. Contingency plan
- B. Continuity of Operations Plan
- C. Disaster recovery plan
- D. Business continuity plan

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 50

Which of the following is a formula, practice, process, design, instrument, pattern, or compilation of information which is not generally known, but by which a business can obtain an economic advantage over its competitors?

- A. Utility model
- B. Cookie
- C. Copyright
- D. Trade secret

Answer: D ([LEAVE A REPLY](#))

Explanation

NEW QUESTION: 51

Which of the following options is an approach to restricting system access to authorized users?

- A. DAC
- B. MIC
- C. RBAC
- D. MAC

Answer: C ([LEAVE A REPLY](#))

Role-based access control (RBAC) is an approach to restricting system access to authorized users. It is a newer alternative approach to mandatory access control (MAC) and discretionary access control (DAC). RBAC is sometimes referred to as role-based security. RBAC is a policy neutral and flexible access control technology sufficiently powerful to simulate DAC and MAC.

Conversely, MAC can simulate RBAC if the role graph is restricted to a tree rather than a partially ordered set. Answer option A is incorrect. Discretionary access control (DAC) is a kind of access control defined by the Trusted Computer System Evaluation Criteria as "a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission on to any other subject".

Answer option D is incorrect. Mandatory access control (MAC) refers to a type of access control by which the operating system constrains the ability of a subject or initiator to access or generally perform some sort of operation on an object or target. In practice, a subject is usually a process or thread; objects are constructs such as files, directories, TCP/UDP ports, shared memory segments, etc. Subjects and objects each have a set of security attributes. Whenever a subject attempts to access an object, an authorization rule enforced by the

operating system kernel examines these security attributes and decides whether the access can take place. Any operation by any subject on any object will be tested against the set of authorization rules to determine if the operation is allowed.

Answer option B is incorrect. Mandatory Integrity Control (MIC), also called Integrity levels, is a core security feature, introduced in Windows Vista and Windows Server 2008, which adds Integrity Levels (IL) to processes running in a login session. This mechanism is able to selectively restrict the access permissions of certain programs or software components which are considered to be potentially less trustworthy, compared with other software running under the same user account which is more trusted.

Reference: GSLC Course Manual, Contents. "Change Management"

NEW QUESTION: 52

Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

- A. Spoofing
- B. Eavesdropping
- C. Packaging
- D. Shielding

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 53

Which of the following BEST describes the purpose of an "escalation matrix" within an incident response plan?

- A. A pricing table for security tools
- B. A defined structure specifying who must be notified, at what severity threshold, and within what timeframe
- C. A list of vendor contacts unrelated to incidents
- D. A technical network diagram

Answer: B ([LEAVE A REPLY](#))

An escalation matrix ensures the right people (technical leads, management, legal, executives) are notified promptly based on incident severity, avoiding delays or gaps in decision-making authority.

NEW QUESTION: 54

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

- A. TLS
- B. HTTP
- C. SNMP
- D. SSL

Answer: A,D ([LEAVE A REPLY](#))

NEW QUESTION: 55

Drop the appropriate value to complete the formula.



Answer:



Explanation:

A Single Loss Expectancy (SLE) is the value in dollar (\$) that is assigned to a single event.

The SLE can be calculated by the following formula.

$SLE = \text{Asset Value } (\$) \times \text{Exposure Factor (EF)}$

The Exposure Factor (EF) represents the % of assets loss caused by a threat.

The EF is required to calculate the Single Loss Expectancy (SLE).

The Annualized Loss Expectancy (ALE) can be calculated by multiplying the Single Loss Expectancy (SLE) with the Annualized Rate of Occurrence (ARO).

$\text{Annualized Loss Expectancy (ALE)} = \text{Single Loss Expectancy (SLE)} \times \text{Annualized Rate of Occurrence (ARO)}$

Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency in which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur.

Reference: "http://en.wikipedia.org/wiki/Risk_management"

NEW QUESTION: 56

Which of the following response teams aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large?

- A. CERT
- B. FIRST
- C. CSIRT
- D. FedCIRC

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 57

Which of the following protocols are used to provide secure communication between a client and a server over the Internet? Each correct answer represents a part of the solution. Choose two.

- A. TLS

- B. HTTP
- C. SNMP
- D. SSL

Answer: A,D ([LEAVE A REPLY](#))

SSL and TLS protocols are used to provide secure communication between a client and a server over the Internet.

NEW QUESTION: 58

During an incident, which role is typically responsible for making the final decision to invoke the disaster recovery plan?

- A. Help desk technician
- B. Emergency management team / senior management
- C. Software team
- D. Off-site storage team

Answer: B ([LEAVE A REPLY](#))

Plan invocation is a business decision made by those with authority over organizational impact, typically emergency management or senior leadership, not technical teams who execute the response.

NEW QUESTION: 59

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?

- A. WinHex
- B. FAR system
- C. Device Seizure
- D. Vedit

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 60

Which of the following is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems?

- A. IDS
- B. OPSEC
- C. HIDS
- D. NIDS

Answer: B ([LEAVE A REPLY](#))

OPSEC (Operations Security) is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, and if information obtained by adversaries could be interpreted to be useful to them. After obtaining the information, the process executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

Answer option C is incorrect. A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyses the internals of a computing system rather than the network packets on its external interfaces. A host-based Intrusion Detection System (HIDS) monitors all or parts of the dynamic behavior and the state of a computer system. HIDS look at the state of a system, its stored information, whether in RAM, in the file system, log files or elsewhere; and check that the contents of these appear as expected.

Answer option A is incorrect. An Intrusion detection system (IDS) is used to detect unauthorized attempts to access and manipulate computer systems locally or through the Internet or an intranet. It can detect several types of attacks and malicious behaviors that can

compromise the security of a network and computers. This includes network attacks against vulnerable services, unauthorized logins and access to sensitive data, and malware (e.g. viruses, worms, etc.). An IDS also detects attacks that originate from within a system. In most cases, an IDS has three main components:

Sensors, Console, and Engine. Sensors generate security events. A console is used to alert and control sensors and to monitor events. An engine is used to record events and to generate security alerts based on received security events. In many IDS implementations, these three components are combined into a single device. Basically, following two types of IDS are used.

Network-based IDS

Host-based IDS

Answer option D is incorrect. A network intrusion detection system (NIDS) is an intrusion detection system that tries to detect malicious activity such as denial of service attacks, port scans or even attempts to crack into computers by monitoring network traffic. A NIDS reads all the incoming packets and tries to find suspicious patterns known as signatures or rules. It also tries to detect incoming shell codes in the same manner that an ordinary intrusion detection systems does.

NEW QUESTION: 61

Which of the following is the BEST description of "impact tolerance" as distinguished from "risk appetite"?

- A. They are identical concepts
- B. Risk appetite is the amount of risk an organization is willing to pursue; impact tolerance is the maximum level of disruption to a specific critical service the organization can absorb before causing intolerable harm
- C. Impact tolerance only applies to financial institutions
- D. Risk appetite is set by regulators, not the organization

Answer: B ([LEAVE A REPLY](#))

Risk appetite is a broader strategic concept about risk-taking generally, while impact tolerance (increasingly used in operational resilience regulation, e.g., UK/EU frameworks) sets a specific outer limit for disruption to an important business service.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 62

You are an Incident manager in Orangesect.Inc. You have been tasked to set up a new extension of your enterprise. The networking, to be done in the new extension, requires different types of cables and an appropriate policy that will be decided by you. Which of the following stages in the Incident handling process involves your decision making?

- A. Preparation
- B. Eradication
- C. Identification
- D. Containment

Answer: A ([LEAVE A REPLY](#))

The preparation phase of the Incident handling process is responsible for defining rules, collaborating human workforce, creating a back-up plan, and testing the plans for an enterprise.

Preparation is the phase of the Incident handling, which involves different processes that are as follows:

Establishing applicable policies

Building relationships with key players

Building a response kit

Establish communication plan

Creating incident checklists

Performing threat modeling

Building an incident response team

Answer option C is incorrect. The Identification phase of the Incident handling process is the stage at which the Incident handler evaluates the critical level of an incident for an enterprise or system. It is an important stage where the distinction between an event and an incident is determined, measured and tested.

Answer option D is incorrect. The Containment phase of the Incident handling process is responsible for supporting and building up the incident combating process. It ensures the stability of the system and also confirms that the incident does not get any worse. The Containment phase includes the process of preventing further contamination of the system or network, and preserving the evidence of the contamination.

Answer option B is incorrect. The Eradication phase of the Incident handling process involves the cleaning-up of the identified harmful incidents from the system. It includes the analyzing of the information that has been gathered for determining how the attack was committed. To prevent the incident from happening again, it is vital to recognize how it was conceded out so that a prevention technique is applied.

Reference: <http://www.giac.org/resources/whitepaper/network/17.php>

NEW QUESTION: 63

Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

A. Third Code of Ethics Canons

B. First Code of Ethics Canons

C. Second Code of Ethics Canons

D. Fourth Code of Ethics Canons

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 64

You work as a Network Administrator for ABC Inc. The company uses a secure wireless network. John complains to you that his computer is not working properly. What type of security audit do you need to conduct to resolve the problem?

A. Independent audit

B. Dependent audit

C. Non-operational audit

D. Operational audit

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 65

You work as a Forensic Investigator. Which of the following rules will you follow while working on a case? Each correct answer represents a part of the solution. Choose all that apply.

- A. Examine original evidence and never rely on the duplicate evidence.
- B. Never exceed the knowledge base of the forensic investigation.
- C. Follow the rules of evidence and never temper with the evidence.
- D. Prepare a chain of custody and handle the evidence carefully.

Answer: A,B,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 66

Which of the following plans provides procedures for recovering business operations immediately following a disaster?

- A. Business continuity plan
- B. Disaster recovery plan
- C. Continuity of operation plan
- D. Business recovery plan

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 67

Which of the following roles typically has ultimate accountability for an organization's overall risk management program, even though day-to-day execution is delegated?

- A. Security analyst
- B. Board of Directors / senior executive management
- C. Help desk manager
- D. External auditor

Answer: B ([LEAVE A REPLY](#))

While execution is delegated to risk and security teams, ultimate accountability for organizational risk oversight rests with the board and senior executive leadership under corporate governance principles.

NEW QUESTION: 68

Which of the following terms related to risk management represents the estimated frequency at which a threat is expected to occur?

- A. Safeguard
- B. Single Loss Expectancy (SLE)
- C. Exposure Factor (EF)
- D. Annualized Rate of Occurrence (ARO)

Answer: D ([LEAVE A REPLY](#))

The Annualized Rate of Occurrence (ARO) is a number that represents the estimated frequency at which a threat is expected to occur. It is calculated based upon the probability of the event occurring and the number of employees that could make that event occur. Answer option C is incorrect. The Exposure Factor (EF) represents the % of assets loss caused by a threat. The EF is required to calculate the Single Loss Expectancy (SLE). Answer option B is incorrect. The Single Loss Expectancy (SLE) is the value in dollars that is assigned to a single event.

$$\text{SLE} = \text{Asset Value (\$)} \times \text{Exposure Factor (EF)}$$

Answer option A is incorrect. Safeguard acts as a countermeasure for reducing the risk associated with a specific threat or a group of threats.

Reference: "http://en.wikipedia.org/wiki/Risk_management"

NEW QUESTION: 69

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

- A. The IT Service Continuity Manager
- B. The Configuration Manager
- C. The Service Catalogue Manager
- D. The Supplier Manager

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 70

You are documenting your organization's change control procedures for project management. What portion of the change control process oversees features and functions of the product scope?

- A. Configuration management
- B. Product scope management is outside the concerns of the project.
- C. Project integration management
- D. Scope changecontrol system

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 71

You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when conducting a security awareness campaign?

- A. Provide customizedmessages for different groups.
- B. Provide technical details on exploits.
- C. Target senior managers and business process owners.
- D. Target system administrators and the help desk.

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 72

Mark works as a security manager for SofTech Inc. He is working in a partially equipped office space which contains some of the system hardware, software, telecommunications, and power sources. In which of the following types of office sites is he working?

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

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 73

Peter works as a Computer Hacking Forensic Investigator. He has been called by an organization to conduct a seminar to give necessary information related to sexual harassment within the work place. Peter started with the definition and types of sexual harassment. He then wants to convey that it is important that records of the sexual harassment incidents should be maintained, which helps in further legal prosecution. Which of the following data should be recorded in this documentation? Each correct answer represents a complete solution. Choose all that apply.

- A. Date and time of incident
- B. Nature of harassment
- C. Location of each incident
- D. Names of the victims

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 74

Which of the following BEST describes "safe harbor" provisions in the context of data breach notification laws?

- A. Safe harbor provisions eliminate all notification requirements
- B. Safe harbor provisions may exempt an organization from notification requirements if specific conditions are met (e.g., data was encrypted)
- C. Safe harbor only applies to government agencies
- D. Safe harbor provisions apply universally regardless of circumstances

Answer: B ([LEAVE A REPLY](#))

Many breach notification laws include safe harbor exceptions - commonly, if compromised data was strongly encrypted and keys were not also compromised, notification obligations may be reduced or waived.

NEW QUESTION: 75

Which of the following is the PRIMARY purpose of an "Acceptable Use Policy (AUP)"?

- A. To define network IP addressing schemes
- B. To define permitted and prohibited use of organizational IT resources by employees/users
- C. To specify vendor SLA terms
- D. To document disaster recovery procedures

Answer: ([SHOW ANSWER](#))

An AUP sets expectations and rules for how employees may use company systems, networks, and data, and is typically acknowledged during onboarding.

NEW QUESTION: 76

Which of the following BEST describes the purpose of "alternate work-site strategies" (e.g., remote work) as part of business continuity for personnel disruptions (e.g., pandemic)?

- A. Alternate work-site planning applies only to IT disruptions, not personnel
- B. Ensuring staff can continue critical functions remotely when a facility is inaccessible or a health crisis prevents on-site work
- C. Alternate work-site strategies eliminate the need for DR planning
- D. Remote work strategies are irrelevant to BCP

Answer: B ([LEAVE A REPLY](#))

BCP must address disruptions to people, not just technology or facilities - pandemic-era planning demonstrated the need for remote work capability as a continuity strategy for personnel-based disruptions.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 77

Which of the following fields of management focuses on establishing and maintaining consistency of a system's or product's performance and its functional and physical attributes with its requirements, design, and operational information throughout its life?

- A. Risk management
- B. Configuration management
- C. Procurement management
- D. Change management

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 78

You are the project manager of the HJK Project for your organization. You and the project team have created risk responses for many of the risk events in the project. Where should you document the proposed responses and the current status of all identified risks?

- A. Risk management plan
- B. Lessons learned documentation
- C. Risk register
- D. Stakeholder management strategy

Answer: C ([LEAVE A REPLY](#))

Risks and the corresponding responses are documented in the risk register for the project. Risk register is a document that contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning.

Description, category, cause, probability of occurring, impact on objectives, proposed responses, owner, and the current status of all identified risks are put in the risk register. Answer option B is incorrect. The outcome of risk events and the corresponding risk responses may be documented in the project's lessons learned documented, but the best answer is to document the risk responses as part of the risk register.

Answer option A is incorrect. The risk management plan defines how risks will be identified and analyzed, the available responses, and the monitoring and controlling of the risk events. The actual risk responses are included in the risk register.

Answer option D is incorrect. The stakeholder management strategy defines how stakeholders and their threats, perceived threats, opinions, and influence over the project objectives will be addressed and managed.

Reference: "Project Management Body of Knowledge (PMBOK Guide), Fourth Edition"

NEW QUESTION: 79

Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

- A. False accusations
- B. Encouraging others to harass the victim
- C. Attempts to gather information about the victim
- D. False victimization

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 80

Which of the following statements reflect the 'Code of Ethics Preamble' in the '(ISC)2 Code of Ethics'? Each correct answer represents a complete solution. Choose all that apply.

- A. Provide diligent and competent service to principals.
- B. Strict adherence to this Code is a condition of certification.
- C. Advance and protect the profession.
- D. Safety of the commonwealth, duty to our principals, and to each other requires that we adhere, and be seen to adhere, to the highest ethical standards of behavior.

Answer: B,D ([LEAVE A REPLY](#))

NEW QUESTION: 81

Which of the following steps are generally followed in computer forensic examinations? Each correct answer represents a complete solution. Choose three.

- A. Acquire
- B. Encrypt
- C. Authenticate
- D. Analyze

Answer: A,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 82

Which of the following BEST describes the relationship between "compliance" and "security"?

- A. Compliance and security are always identical - being compliant guarantees being secure
- B. Compliance establishes a regulatory/legal baseline, but true security requires managing risk beyond minimum compliance requirements
- C. Security is a subset of compliance with no independent value
- D. Compliance is irrelevant to a mature security program

Answer: (SHOW ANSWER)

A well-known ISSMP theme: "compliant does not mean secure." Regulatory compliance sets a necessary floor, but organizations must manage risk holistically, which often requires controls beyond minimum legal/regulatory requirements.

NEW QUESTION: 83

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

- A. MS-CHAP v2
- B. CHAP
- C. PAP
- D. EAP

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 84

Which of the following is a variant with regard to Configuration Management?

- A. A CI that has the same essential functionality as another CI but a bit different in some small manner.
- B. A CI that particularly refers to a software version.
- C. A CI that has the same name as another CI but shares no relationship.
- D. A CI that particularly refers to a hardware specification.

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 85

Which of the following BEST captures the ISSMP's overarching emphasis when synthesizing across ALL its domains (Leadership, Threat Intelligence, Risk, Security Planning, Contingency Management, Law/Ethics)?

- A. Deep, narrow technical specialization in a single tool or technology
- B. The ability to lead and integrate people, process, technology, legal, and business considerations into a cohesive, risk-informed security management strategy
- C. Strict adherence to checklists without contextual judgment
- D. Delegating all strategic decisions to technical staff

Answer: ([SHOW ANSWER](#))

Across every domain, ISSMP consistently emphasizes integrative leadership - connecting technical risk with business strategy, legal obligation, organizational culture, and crisis management - rather than deep technical execution in any single area, reflecting its identity as a senior management/leadership credential.

NEW QUESTION: 86

Which of the following are the process steps of OPSEC? Each correct answer represents a part of the solution. Choose all that apply.

- A. Analysis of Vulnerabilities
- B. Identification of Critical Information
- C. Display of associated vulnerability components
- D. Assessment of Risk

Answer: A,B,D ([LEAVE A REPLY](#))

NEW QUESTION: 87

Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

- A. Artistic license
- B. Phishing
- C. Patent
- D. Spam

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 88

Which of the following BEST describes the concept of "security champions" embedded within business/development teams?

- A. Individuals who replace the need for a centralized security function
- B. Team members who receive additional security training and act as liaisons, promoting security awareness and practices within their local team
- C. Security champions have no defined role or responsibility
- D. Security champions are only relevant in large enterprises

Answer: B ([LEAVE A REPLY](#))

Security champion programs extend the security team's reach by embedding security-minded advocates within business/development teams, improving early identification of issues and cultural adoption of secure practices.

NEW QUESTION: 89

Fill in the blank with an appropriate phrase. _____ is a branch of forensic science pertaining to legal evidence found in computers and digital storage media.

- A. Computer forensics

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 90

Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

- A. EAP
- B. PAP
- C. MS-CHAP v2
- D. CHAP

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 91

Which of the following BEST describes why "third-party breach notification clauses" are important in vendor contracts?

- A. They are irrelevant since vendors are solely liable for their own breaches
- B. They obligate the vendor to promptly inform the organization of a breach affecting shared/processed data, enabling timely response and regulatory compliance
- C. They eliminate the need for a vendor risk assessment
- D. They only apply to cloud vendors

Answer: B ([LEAVE A REPLY](#))

Since the client organization often retains regulatory notification obligations (e.g., under GDPR) even when a vendor is breached, contracts must require prompt vendor notification to enable the client to meet its own compliance timelines.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 92

Which of the following governance bodies provides management, operational and technical controls to satisfy security requirements?

- A. Senior Management
- B. Business Unit Manager
- C. Information Security Steering Committee
- D. Chief Information Security Officer

Answer: A ([LEAVE A REPLY](#))

Senior management provides management, operational and technical controls to satisfy security requirements. The governance roles and responsibilities are mentioned below in the table.

NEW QUESTION: 93

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.C. 2510
- B. 18 U.S. 1029
- C. 18 U.S.C. 1030
- D. 18 U.S.C. 1362
- E. 18 U.S.C. 2701

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 94

Which of the following laws is defined as the Law of Nations or the legal norms that has developed through the customary exchanges between states over time, whether based on diplomacy or aggression?

- A. Administrative
- B. Customary
- C. Criminal
- D. Tort

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 95

Which of the following BEST describes the purpose of "segregation of duties" combined with "job rotation" as complementary controls?

- A. They serve no combined purpose
- B. Together they reduce the risk of undetected fraud by limiting single-person control and periodically exposing hidden irregularities
- C. Job rotation replaces the need for segregation of duties
- D. These controls apply only to executive staff

Answer: (SHOW ANSWER)

Segregation of duties limits any one person's control over a complete process; job rotation adds a detective element by periodically placing different people into roles, increasing the chance that irregularities are discovered.

NEW QUESTION: 96

John works as a security manager for Soft Tech Inc. He is working with his team on the disaster recovery management plan. One of his team members has a doubt related to the most cost effective DRP testing plan. According to you, which of the following disaster recovery testing plans is the most cost-effective and efficient way to identify areas of overlap in the plan before conducting more demanding training exercises?

- A. Full-scale exercise
- B. Walk-through drill
- C. Evacuation drill
- D. Structured walk-through test

Answer: D (LEAVE A REPLY)

NEW QUESTION: 97

Management has asked you to perform a risk audit and report back on the results. Bonny, a project team member asks you what a risk audit is. What do you tell Bonny?

- A. A risk audit is a review of the effectiveness of the risk responses in dealing with identified risks and their root causes, as well as the effectiveness of the risk management process.
- B. A risk audit is a review of all the risk probability and impact for the risks, which are still present in the project but which have not yet occurred.
- C. A risk audit is a review of all the risks that have yet to occur and what their probability of happening are.
- D. A risk audit is an audit of all the risks that have occurred in the project and what their true impact on cost and time has been.

Answer: A (LEAVE A REPLY)

NEW QUESTION: 98

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.C. 1362
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 1029
- D. 18 U.S.C. 2701
- E. 18 U.S.C. 2510

Answer: A (LEAVE A REPLY)

The 18 U.S.C. 1362 law is related to computer crime activities in communication lines, stations, or systems.

Answer option C is incorrect. The 18 U.S.C. 1029 law addresses fraud and related activities in connection with access devices.

Answer option B is incorrect. The 18 U.S.C. 1030 law addresses fraud and related activities in connection with computers.

Answer option E is incorrect. The 18 U.S.C. 2510 law addresses computer crime activities related to wires and electronic communication interceptions and interceptions of oral communication.

Answer option D is incorrect. The 18 U.S.C. 2701 law addresses computer crime activities related to both stored wires and electronic communication interceptions and interceptions of oral communication.

Reference: <http://www.cybercrime.gov/cclaws.html>

NEW QUESTION: 99

Which of the following types of agreement creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret?

- A. SLA
- B. NDA
- C. Non-price competition
- D. CNC

Answer: B ([LEAVE A REPLY](#))

A non-disclosure agreement (NDA) is a legal contract between at least two parties that outlines confidential materials or knowledge the parties wish to share with one another for certain purposes, but wish to restrict access to. It is a contract through which the parties agree not to disclose information covered by the agreement. An NDA creates a confidential relationship between the parties to protect any type of confidential and proprietary information or a trade secret. Answer option D is incorrect. A non-compete clause or covenant not to compete (CNC), is a term used in contract law under which one party (usually an employee) agrees to not pursue a similar profession or trade in competition against another party (usually the employer). Answer option A is incorrect. A service-level agreement (SLA) is a negotiated agreement between two parties where one is the customer and the other is the service provider. It records a common understanding about services, priorities, responsibilities, guarantees, and warranties. Each area of service scope should have the 'level of service' defined. The SLA may specify the levels of availability, serviceability, performance, operation, or other attributes of the service such as billing.

Answer option C is incorrect. Non-price competition is a marketing strategy in which one firm tries to distinguish its product or service from competing products on the basis of attributes like design and workmanship.

NEW QUESTION: 100

You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

- A. Availability
- B. Encryption
- C. Integrity
- D. Confidentiality

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 101

Which of the following divisions of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy?

- A. Division B
- B. Division A
- C. Division D
- D. Division C

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 102

Which of the following types of activities can be audited for security? Each correct answer represents a complete solution. Choose three.

- A. Data downloading from the Internet
- B. Network logons and logoffs
- C. File and object access
- D. Printer access

Answer: B,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 103

Which of the following BEST reflects the concept of "management commitment" as a critical success factor in ISSMP-aligned security programs?

- A. Security programs succeed based on technology alone
- B. Visible executive sponsorship, resourcing, and support are essential for a security program's effectiveness and cultural adoption
- C. Management involvement is only needed during audits
- D. Security programs should operate independently of business leadership

Answer: B ([LEAVE A REPLY](#))

A recurring ISSMP theme is that security governance and culture require sustained executive sponsorship - without it, policies lack authority, funding, and organizational buy-in.

NEW QUESTION: 104

Sarah has created a site on which she publishes a copyrighted material. She is ignorant that she is infringing copyright. Is she guilty under copyright laws?

- A. Yes
- B. No

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 105

Which of the following strategies is used to minimize the effects of a disruptive event on a company, and is created to prevent interruptions to normal business activity?

- A. Continuity of Operations Plan
- B. Business Continuity Plan
- C. Contingency Plan
- D. Disaster Recovery Plan

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 106

Which of the following signatures watches for the connection attempts to well-known, frequently attacked ports?

- A. Digital signatures
- B. Port signatures
- C. String signatures
- D. Header condition signatures

Answer: B ([LEAVE A REPLY](#))

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:
<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 107

You are the Network Administrator for a software company. Due to the nature of your company's business, you have a significant number of highly computer savvy users. However, you have still decided to limit each user access to only those resources required for their job, rather than give wider access to the technical users (such as tech support and software engineering personnel).

What is this an example of?

- A.** The principle of maximum control.
- B.** The principle of least privileges.
- C.** Proper use of an ACL.
- D.** Poor resource management.

Answer: B ([LEAVE A REPLY](#))

No matter how technically proficient the users are, it is always proper for an administrator to grant each user the least/lowest privileges possible for them to do their job (thus the term least privileges). You should never grant any user any more access than they require to perform their job functions.

Answer option D is incorrect. This is absolutely not poor resource management, but rather wise security policy, thus wise resource management.

Answer option A is incorrect. The term 'maximum control' is not a valid network security term.

Answer option C is incorrect. An ACL or access control list is used to control access to resources by matching a user on the list with rights to a resource. This may or may not have the user with more access than their job requires.

Reference: "<https://buildsecurityin.us-cert.gov/daisy/bsi/articles/knowledge/principles/351-BSI.html>"

NEW QUESTION: 108

Which of the following security models focuses on data confidentiality and controlled access to classified information?

- A.** Bell-La Padula model
- B.** Take-Grant model
- C.** Clark-Wilson model
- D.** Biba model

Answer: A ([LEAVE A REPLY](#))

The Bell-La Padula Model is a state machine model used for enforcing access control in government and military applications. The model is a formal state transition model of computer security policy that describes a set of access control rules which use security labels on objects and clearances for subjects. Security labels range from the most sensitive (e.g., "Top Secret"), down to the least sensitive (e.g., "Unclassified" or "Public").

The Bell-La Padula model focuses on data confidentiality and controlled access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.

Answer option D is incorrect. The Biba model is a formal state transition system of computer security policy that describes a set of access control rules designed to ensure data integrity. Data and subjects are grouped into ordered levels of integrity. The model is designed so that subjects may not corrupt data in a level ranked higher than the subject, or be corrupted by data from a lower level than the subject.

Answer option C is incorrect. The Clark-Wilson model provides a foundation for specifying and analyzing an integrity policy for a computing system. The model is primarily concerned with formalizing the notion of information integrity. Information integrity is maintained by preventing corruption of data items in a system due to either error or malicious intent. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy. The core of the model is based on the notion of a transaction. The model's enforcement and certification rules define data items and processes that provide the basis for an integrity policy.

The core of the model is based on the notion of a transaction. Answer option B is incorrect. The take-grant protection model is a formal model used in the field of computer security to establish or disprove the safety of a given computer system that follows specific rules. It shows that for specific systems the question of safety is decidable in linear time, which is in general undecidable.

The model represents a system as directed graph, where vertices are either subjects or objects.

The edges between them are labeled and the label indicates the rights that the source of the edge has over the destination. Two rights occur in every instance of the model: take and grant.

They play a special role in the graph rewriting rules describing admissible changes of the graph.

NEW QUESTION: 109

Which of the following BEST describes the PRIMARY value of scenario-based planning (e.g., "what if a ransomware attack encrypts our ERP system") in security management?

- A.** It is purely a theoretical academic exercise
- B.** It helps identify gaps in plans, roles, and capabilities before a real event occurs, improving preparedness
- C.** It replaces the need for a documented incident response plan
- D.** It is only useful for physical disaster scenarios

Answer: ([SHOW ANSWER](#))

Scenario planning stress-tests existing plans against realistic, specific threats, surfacing gaps in technical capability, communication, or authority that might not be evident from generic planning alone.

NEW QUESTION: 110

Which of the following BEST describes why an organization should maintain a documented "incident response playbook" for specific threat scenarios (e.g., ransomware, business email compromise)?

- A.** Generic incident response plans are always sufficient for every scenario
- B.** Scenario-specific playbooks provide detailed, pre-defined action steps tailored to common attack types, improving response speed and consistency
- C.** Playbooks eliminate the need for analyst judgment entirely
- D.** Playbooks are only useful for compliance audits, not actual response

Answer: **B** ([LEAVE A REPLY](#))

While a general IR plan covers overall process, scenario-specific playbooks (e.g., for ransomware, BEC, DDoS) provide detailed technical and procedural steps tailored to that threat type, enabling faster, more consistent response.

NEW QUESTION: 111

Shoulder surfing is a type of in-person attack in which the attacker gathers information about the premises of an organization. This attack is often performed by looking surreptitiously at the keyboard of an employee's computer while he is typing in his password at any access point such as a terminal/Web site. Which of the following is violated in a shoulder surfing attack?

- A. Availability
- B. Confidentiality
- C. Integrity
- D. Authenticity

Answer: [\(SHOW ANSWER\)](#)

Confidentiality is violated in a shoulder surfing attack. The CIA triad provides the following three tenets for which security practices are measured.

Confidentiality. It is the property of preventing disclosure of information to unauthorized individuals or systems. Breaches of confidentiality take many forms. Permitting someone to look over your shoulder at your computer screen while you have confidential data displayed on it could be a breach of confidentiality. If a laptop computer containing sensitive information about a company's employees is stolen or sold, it could result in a breach of confidentiality. Integrity. It means that data cannot be modified without authorization. Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an unauthorized user vandalizes a web site, when someone is able to cast a very large number of votes in an online poll, and so on.

Availability. It means that data must be available at every time when it is needed. Answer option D is incorrect. Authenticity is not a tenet of the CIA triad.

NEW QUESTION: 112

Which of the following is generally considered the WEAKEST basis for making a risk acceptance decision?

- A. Formal risk assessment with quantified impact and likelihood
- B. Gut feeling of an individual manager without documented analysis
- C. Business impact analysis results
- D. Cost-benefit analysis of controls

Answer: [B \(LEAVE A REPLY\)](#)

ISSMP emphasizes structured, documented, and justifiable risk decisions; undocumented subjective judgment lacks accountability and traceability, which is problematic for governance and audit purposes.

NEW QUESTION: 113

Which of the following 'Code of Ethics Canons' of the '(ISC)2 Code of Ethics' states to act honorably, honestly, justly, responsibly and legally?

- A. Fourth Code of Ethics Canons
- B. Third Code of Ethics Canons
- C. Second Code of Ethics Canons
- D. First Code of Ethics Canons

Answer: [C \(LEAVE A REPLY\)](#)

NEW QUESTION: 114

Which of the following roles is used to ensure that the confidentiality, integrity, and availability of the services are maintained to the levels approved on the Service Level Agreement (SLA)?

- A. The Service Level Manager
- B. The Configuration Manager
- C. The IT Security Manager
- D. The Change Manager

Answer: ([SHOW ANSWER](#))

The IT Security Manager is responsible for ensuring the confidentiality, integrity, and availability of an organization's assets, information, data, and IT services. He is usually involved in an organizational approach to Security Management, which has a wider scope than the IT service provider, and includes handling of paper, building access, phone calls, etc for the entire organization. Answer option D is incorrect. The Change Manager authorizes and documents all changes in the IT Infrastructure and its components (Configuration Items), in order to maintain a minimum amount of interruptive effects upon the running operation. In the case of further- reaching changes, he involves the Change Advisory Board (CAB).

Answer option A is incorrect. The Service Level Manager is responsible for negotiating Service Level Agreements and ensuring that these are met. He makes sure that all IT Service Management processes, Operational Level Agreements, and Underpinning Contracts are appropriate for the agreed service level targets. The Service Level Manager also monitors and reports on service levels.

Answer option B is incorrect. The Configuration Manager is responsible for maintaining information about Configuration Items (CI) required to deliver IT services. To this end he maintains a logical model, containing the components of the IT infrastructure (CIs) and their associations.

Reference: ITIL v3 Study Guide, Published with the permission of the Office of Government Commerce (OGC)

NEW QUESTION: 115

Rick is the project manager for TTM project. He is in the process of procuring services from vendors. He makes a contract with a vendor in which he precisely specify the services to be procured, and any changes to the procurement specification will increase the costs to the buyer.

Which type of contract is this?

- A. Firm Fixed Price
- B. Fixed Price Incentive Fee
- C. Cost Plus Fixed Fee Contract
- D. Fixed Price with Economic Price Adjustment

Answer: A ([LEAVE A REPLY](#))

Rick has prepared a Firm Fixed Price contract (FFP). In such contracts, the buyer must precisely specify the product or services to be procured, and any changes to the procurement specification can increase the costs to the buyer. This is the most commonly used contract type. Answer option B is incorrect. In Firm Price Incentive Fee (FPIF) contracts, a price ceiling is set, and all costs above the price ceiling are the responsibility of the seller, who is obligated to complete the work.

Answer option D is incorrect. Fixed Price with Economic Price Adjustment (FP-EPA) is intended to protect both buyer and seller from external conditions beyond their control. Answer option C is incorrect. Cost Plus Fixed Fee Contracts charge back all project costs to the seller and include a fixed fee upon completion of the contracts.

Reference: "A Guide to the Project Management Body of Knowledge, (PMBOK Guide), Fourth Edition."

NEW QUESTION: 116

Which of the following BEST describes a "false positive" in the context of security monitoring, and its management implication?

- A. A real attack that went undetected
- B. An alert indicating malicious activity when none actually occurred, which can waste analyst resources and cause alert fatigue if excessive
- C. A false positive always indicates a system failure
- D. False positives have no operational cost

Answer: ([SHOW ANSWER](#))

Excessive false positives consume analyst time and can lead to "alert fatigue," where real threats may be missed among noise - a key operational tuning concern for SOC management.

NEW QUESTION: 117

Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

- A. Shielding
- B. Spoofing
- C. Eavesdropping
- D. Packaging

Answer: ([SHOW ANSWER](#))

Eavesdropping is the process of listening in private conversations. It also includes attackers listening in on the network traffic. For example, it can be done over telephone lines (wiretapping), e-mail, instant messaging, and any other method of communication considered private. Answer option B is incorrect. Spoofing is a technique that makes a transmission appear to have come from an authentic source by forging the IP address, email address, caller ID, etc. In IP spoofing, a hacker modifies packet headers by using someone else's IP address to hide his identity.

However, spoofing cannot be used while surfing the Internet, chatting on-line, etc. because forging the source IP address causes the responses to be misdirected.

Answer option A is incorrect. Shielding cannot be done over e-mail and instant messaging.

Shielding is a way of preventing electronic emissions that are generated from a computer or network from being used by unauthorized users for gathering confidential information. It minimizes the chances of eavesdropping within a network. Shielding can be provided by surrounding a computer room with a Farady cage. A Farady cage is a device that prevents electromagnetic signal emissions from going outside the computer room. Shielding can also protect wireless networks from denial of service (DoS) attacks.

Answer option D is incorrect. Packaging is a process in which goods are differentiated on the basis of the container in which they are stored, such as bottles, boxes, bags, etc.

Reference: "<http://en.wikipedia.org/wiki/Eavesdropping>"

NEW QUESTION: 118

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models?

Each correct answer represents a complete solution. Choose all that apply.

- A. Performing quality control
- B. Recreating and analyzing the problem
- C. Developing the changes and corresponding tests
- D. Establishing the priorities of requests

Answer: A,B,C (LEAVE A REPLY)

The subphases of the maintenance phase in the life cycle model are as follows:

Request control: This phase manages the users' requests for changes to the software product and gathers information that can be used for managing this activity. Change control: This phase is the most important step in the maintenance phase. Various issues are addressed by the change control phase. Some of them are as follows :

- 1.Recreating and analyzing the problem
- 2.Developing the changes and corresponding tests
- 3.Performing quality control

Release control: It is associated with issuing the latest release of the software. Release control phase involves deciding which requests will be included in the new release, archiving of the release, configuration management, quality control, distribution, and acceptance testing. Answer option D is incorrect. This is a step performed in the request control phase.

Reference: CISM Review Manual 2010, Contents: "Information security process management"

NEW QUESTION: 119

Which of the following BEST describes why security program budgets should be justified using risk-based business cases rather than fear-based appeals?

- A.** Fear-based appeals are always more effective with executives
- B.** Risk-based justification ties investment to quantifiable business risk reduction, supporting sustainable executive buy-in and resource allocation
- C.** Budget justification is not part of a CISO's responsibilities
- D.** Business cases are unnecessary if the CISO has executive trust

Answer: B (LEAVE A REPLY)

Sustainable security funding requires demonstrating value in business terms (risk reduction, cost avoidance, enabling business objectives) rather than relying on fear, uncertainty, and doubt (FUD), which erodes credibility over time.

NEW QUESTION: 120

Configuration Management (CM) is an Information Technology Infrastructure Library (ITIL) IT Service Management (ITSM) process.

Configuration Management is used for which of the following? 1.To account for all IT assets 2.To provide precise information support to other ITIL disciplines 3.To provide a solid base only for Incident and Problem Management 4.To verify configuration records and correct any exceptions

- A.** 1, 3, and 4 only
- B.** 2 and 4 only
- C.** 1, 2, and 4 only
- D.** 2, 3, and 4 only

Answer: C (LEAVE A REPLY)

Explanation/Reference:

NEW QUESTION: 121

Which of the following BEST illustrates the difference between a "Standard Operating Procedure (SOP)" and a "Policy"?

- A.** An SOP provides high-level intent; a policy provides step-by-step tasks
- B.** A policy sets mandatory high-level direction; an SOP provides detailed step-by-step instructions to implement that direction

- C. They are interchangeable terms with no meaningful difference
- D. SOPs are optional while policies are recommendations

Answer: B (LEAVE A REPLY)

Policies establish the "what" and "why" at a high level; SOPs/procedures provide the detailed "how" - the operational steps to comply with policy.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF Special Discount: Exam-Tests**)

NEW QUESTION: 122

Which of the following plans is designed to protect critical business processes from natural or man-made failures or disasters and the resultant loss of capital due to the unavailability of normal business processes?

- A. Disaster recovery plan
- B. Businesscontinuity plan
- C. Crisis communication plan
- D. Contingency plan

Answer: B (LEAVE A REPLY)

NEW QUESTION: 123

Which of the following BEST summarizes the ISSMP view on the CISO's relationship with other C-suite executives (CFO, COO, CIO, General Counsel)?

- A. The CISO should operate independently without cross-functional collaboration
- B. The CISO should build collaborative relationships across the C-suite to embed security into broader business decision-making and risk management
- C. Only the CIO needs to be consulted on security matters
- D. Cross-functional collaboration is only necessary during a breach

Answer: (SHOW ANSWER)

ISSMP emphasizes that effective security leadership requires ongoing collaboration with peer executives - finance, operations, legal, and IT - to ensure security is integrated into strategic decisions rather than operating in isolation.

NEW QUESTION: 124

Which of the following is the PRIMARY purpose of a security metrics dashboard presented to the board of directors?

- A. To show granular technical logs
- B. To communicate security posture and risk in business-relevant, digestible terms
- C. To replace the need for an annual audit
- D. To list every open vulnerability by CVE number

Answer: ([**SHOW ANSWER**](#)**)**

Board-level reporting should translate technical detail into business risk context (trends, exposure, program maturity) rather than raw technical data.

NEW QUESTION: 125

Which of the following BEST describes why "third-party dependency documentation" should be part of the BIA process?

- A.** Third-party dependencies are outside the scope of a BIA
- B.** Understanding which critical business functions rely on external vendors/services helps identify risk exposure and inform recovery/contingency requirements for those dependencies
- C.** Third-party dependencies never affect internal recovery timelines
- D.** BIAs should focus exclusively on internal systems

Answer: ([**SHOW ANSWER**](#)**)**

A comprehensive BIA identifies not just internal system dependencies but also critical external/vendor dependencies, since a vendor's outage can be just as disruptive as an internal system failure - informing vendor SLAs and contingency needs.

NEW QUESTION: 126

Which of the following is the PRIMARY goal of a post-incident review meeting involving legal, HR, and security teams?

- A.** To publicly shame the responsible employee
- B.** To ensure a comprehensive, cross-functional understanding of the incident and coordinated remediation/compliance response
- C.** To finalize the annual budget
- D.** To conduct routine vulnerability scanning

Answer: ([**SHOW ANSWER**](#)**)**

Significant incidents often have legal, HR, regulatory, and technical dimensions; cross-functional review ensures all angles (liability, employee action, compliance obligations, technical fixes) are addressed.

NEW QUESTION: 127

Which of the following attacks can be mitigated by providing proper training to the employees in an organization?

- A.** Man-in-the-middle
- B.** Social engineering
- C.** Smurf
- D.** Denial-of-Service

Answer: B ([**LEAVE A REPLY**](#)**)**

NEW QUESTION: 128

Which of the following are the major tasks of risk management? Each correct answer represents a complete solution. Choose two.

- A.** Assuring the integrity of organizational data
- B.** Building Risk free systems
- C.** Risk control
- D.** Risk identification

Answer: C,D ([**LEAVE A REPLY**](#)**)**

The following are the two major tasks of risk management:

1.Risk identification

2.Risk control

Risk identification is the task of examining and documenting the security posture of an organization's information technology and the risks it faces.

Risk control is the task of applying controls to reduce risks to an organization's data and information systems.

Answer options B and A are incorrect. Building risk free systems and assuring the integrity of organizational data are the tasks related to the implementation of security measures.

Reference: "http://en.wikipedia.org/wiki/Risk_management"

NEW QUESTION: 129

Which of the following BEST describes "impact analysis" as distinct from "likelihood analysis" in risk assessment?

A. They measure the same thing

B. Impact analysis estimates the severity of consequences if a risk materializes; likelihood analysis estimates the probability that it will occur

C. Impact analysis only applies to financial risk

D. Likelihood analysis is irrelevant once impact is known

Answer: B (LEAVE A REPLY)

Risk = likelihood ? impact. Impact analysis focuses on "how bad" an outcome would be, while likelihood analysis focuses on "how probable" - both dimensions are needed to prioritize risk.

NEW QUESTION: 130

A security governance framework primarily helps ensure which of the following?

A. Technical staff can bypass policy for efficiency

B. Security decisions align with organizational objectives and are subject to appropriate oversight

C. All risk is eliminated

D. Compliance replaces the need for risk management

Answer: (SHOW ANSWER)

Governance frameworks establish accountability, decision rights, and alignment between security activities and business objectives - they don't eliminate risk or replace risk management.

NEW QUESTION: 131

In which of the following mechanisms does an authority, within limitations, specify what objects can be accessed by a subject?

A. Role-Based Access Control

B. Discretionary Access Control

C. Task-based Access Control

D. Mandatory Access Control

Answer: B (LEAVE A REPLY)

In the discretionary access control, an authority, within limitations, specifies what objects can be accessed by a subject.

Answer option D is incorrect. In the mandatory access control, a subject's access to an object is dependent on labels.

Answer option A is incorrect. In the role-based access control, a central authority determines what individuals can have access to which objects based on the individual's role or title in the organization.

Answer option C is incorrect. The task-based access control is similar to role-based access control, but the controls are based on the subject's responsibilities and duties.

Reference: CISM Review Manual 2010, Contents. "Information Security Governance"

NEW QUESTION: 132

You work as a project manager for SoftTech Inc. A threat with a dollar value of \$150,000 is expected to happen in your project and the frequency of threat occurrence per year is 0.001. What will be the annualized loss expectancy in your project?

- A. \$100
- B. \$120
- C. \$180.25
- D. \$150

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 133

Which of the following is the PRIMARY objective of conducting a "privacy impact assessment (PIA)"?

- A. To calculate the financial value of customer data
- B. To identify and mitigate privacy risks associated with a system or process that handles personal data
- C. To replace the need for a security risk assessment
- D. To satisfy marketing department requirements

Answer: ([SHOW ANSWER](#)**)**

A PIA systematically evaluates how personal data is collected, used, stored, and shared, identifying privacy risks and required safeguards - often mandated by regulations like GDPR for high-risk processing.

NEW QUESTION: 134

Which of the following evidences are the collection of facts that, when considered together, can be used to infer a conclusion about the malicious activity/person?

- A. Direct
- B. Circumstantial
- C. Incontrovertible
- D. Corroborating

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 135

Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

- A. Evidence access policy
- B. Incident response policy
- C. Chain of custody
- D. Chain of evidence

Answer: C ([LEAVE A REPLY](#))

A chain of custody is a documentation that shows who has collected and accessed each piece of evidence. The documentation must be meticulously prepared including the minutest details (such as the date, time, location, and the verified identity of every person handling

the evidence) so that the documentation is verifiable. It includes the time of accessing the evidence and the valid reason for doing so. A chain of custody must be maintained for all evidences in order to maintain the validity of the evidences.

Answer option B is incorrect. Incident response policy is a document that defines an incident and helps people to respond appropriately to that incident. It provides information about people who are responsible for handling security incidents and how they can be contacted. The incident response policy also provides instructions to deal with documenting and disseminating incident- related information.

Reference: TechNet, Contents. "Data Security and Data Availability in the Administrative Authority"

NEW QUESTION: 136

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A.** Custodian
- B.** User
- C.** Security auditor
- D.** Owner
- E.** Editor

Answer: A,B,C,D ([LEAVE A REPLY](#))

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 137

Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

- A.** Vulnerability analysis
- B.** Cost-benefit analysis
- C.** Gap analysis
- D.** Requirement analysis

Answer: C ([LEAVE A REPLY](#))

Gap analysis is a tool that helps a company to compare its actual performance with its potential performance. It is a formal study of what a business is doing currently and where it wants to go in the future. Gap analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome.

The goal of gap analysis is to identify the gap between the optimized allocation and integration of the inputs, and the current level of allocation. This helps provide the company with insight into areas, which could be improved. The gap analysis process involves determining, documenting and approving the variance between business requirements and current capabilities. Answer option A is incorrect. Vulnerability analysis is also known as vulnerability assessment. It is a process that defines systematic examination of a critical infrastructure, identifies and classifies the security vulnerabilities in a computer, network, or communications infrastructure. In addition,

vulnerability analysis forecasts the effectiveness of proposed countermeasures, identifies the security deficiencies, evaluates the security alternatives, and verifies the adequacy of such measures after implementation.

Answer option B is incorrect. A cost benefit analysis is a technique related to the cost effectiveness of different alternatives in order to see whether the benefits outweigh the costs. Its aim is to gauge the efficiency of the intervention relative to the status quo.

NEW QUESTION: 138

Which of the following anti-child pornography organizations helps local communities to create programs and develop strategies to investigate child exploitation?

- A.** Internet Crimes Against Children (ICAC)
- B.** Project Safe Childhood (PSC)
- C.** Anti-Child Porn.org
- D.** Innocent Images National Initiative (IINI)

Answer: B ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 139

Which of the following are the common roles with regard to data in an information classification program? Each correct answer represents a complete solution. Choose all that apply.

- A.** Owner
- B.** Custodian
- C.** Security auditor
- D.** User
- E.** Editor

Answer: A,B,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 140

Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

- A.** Gap analysis
- B.** Requirement analysis
- C.** Vulnerability analysis
- D.** Cost-benefit analysis

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 141

Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

- A.** Outsource
- B.** Contract
- C.** Proposal
- D.** Service level agreement

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 142

Your company is covered under a liability insurance policy, which provides various liability coverage for information security risks, including any physical damage of assets, hacking attacks, etc. Which of the following risk management techniques is your company using?

- A. Risk mitigation
- B. Risk transfer
- C. Risk acceptance
- D. Risk avoidance

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 143

Which of the following is used to back up forensic evidences or data folders from the network or locally attached hard disk drives?

- A. Vedit
- B. FAR system
- C. WinHex
- D. Device Seizure

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 144

During a tabletop exercise, participants discuss their roles and responses to a simulated incident without actually activating systems. This is an example of which testing type?

- A. Full interruption test
- B. Parallel test
- C. Structured walkthrough (tabletop) test
- D. Simulation test

Answer: (SHOW ANSWER)

A tabletop/structured walkthrough is a discussion-based exercise where team members review procedures verbally without operational disruption. Answer options A and B involve actual system activity; D typically involves acting out response steps more actively than a tabletop but still short of live systems.

NEW QUESTION: 145

SIMULATION

Fill in the blank with an appropriate phrase. _____ is used to provide security mechanisms for the storage, processing, and transfer of data.

Answer:

Data classification

NEW QUESTION: 146

Which of the following roles is responsible for review and risk analysis of all contracts on a regular basis?

- A. The Configuration Manager

- B. The Supplier Manager
- C. The Service Catalogue Manager
- D. The IT Service Continuity Manager

Answer: ([SHOW ANSWER](#))

The Supplier Manager role is responsible for review and risk analysis of all contracts on a regular basis. The Supplier Manager is responsible for ensuring that value for money is obtained from all suppliers. He makes sure that contracts with suppliers support the needs of the business, and that all suppliers meet their contractual commitments.

Answer option C is incorrect. The Service Catalogue Manager is responsible for maintaining the Service Catalogue, ensuring that all information within the Service Catalogue is accurate and up to date.

Answer option A is incorrect. The Configuration Manager is responsible for maintaining information about Configuration Items that are required to deliver IT services. He also maintains a logical model, containing the components of the IT infrastructure (CIs) and their associations.

Answer option D is incorrect. The IT Service Continuity Manager is responsible for managing risks that could seriously impact IT services. He ensures that the IT service provider can provide minimum agreed service levels in cases of disaster, by reducing the risk to an acceptable level and planning for the recovery of IT services.

Reference: ITIL v3 Study Guide, Published with the permission of the Office of Government Commerce (OGC)

NEW QUESTION: 147

Which of the following BEST describes the concept of "residual risk reporting cadence" as a governance practice?

- A. Residual risk should be reported once at project completion only
- B. Residual risk should be reported to appropriate stakeholders on a defined, recurring basis to ensure it remains visible and periodically re-evaluated
- C. Residual risk reporting is unnecessary once initially accepted
- D. Cadence is irrelevant since residual risk never changes

Answer: B ([LEAVE A REPLY](#))

Risk conditions change over time (new threats, control degradation, business changes); mature governance requires periodic re-reporting and re-evaluation of previously accepted residual risk, not a one-time acceptance that's never revisited.

NEW QUESTION: 148

Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

- A. Integrity
- B. Privacy
- C. Availability
- D. Confidentiality

Answer: A,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 149

Which of the following BEST describes the concept of "graceful degradation" as a resilience design principle?

- A. Systems should fail completely and immediately upon any disruption

B. Systems are designed to continue operating at reduced functionality/capacity rather than failing entirely when a component becomes unavailable

C. Graceful degradation applies only to network hardware

D. Graceful degradation eliminates the need for a DRP

Answer: B (LEAVE A REPLY)

Rather than an all-or-nothing failure mode, resilient systems are designed to shed non-critical functionality while preserving core operations when under stress or partial failure - improving overall availability during disruption.

NEW QUESTION: 150

Which of the following access control models uses a predefined set of access privileges for an object of a system?

A. Role-Based Access Control

B. Mandatory Access Control

C. Policy Access Control

D. Discretionary Access Control

Answer: B (LEAVE A REPLY)

Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission.

Answer option D is incorrect. DAC is an access control model. In this model, the data owner has the right to decide who can access the data.

Answer option A is incorrect. Role-based access control (RBAC) is an access control model. In this model, a user can access resources according to his role in the organization. For example, a backup administrator is responsible for taking backups of important data.

Therefore, he is only authorized to access this data for backing it up. However, sometimes users with different roles need to access the same resources.

This situation can also be handled using the RBAC model. Answer option C is incorrect. There is no such access control model as Policy Access Control.

Reference: "http://en.wikipedia.org/wiki/Mandatory_access_control"

NEW QUESTION: 151

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software. Which of the following SDLC phases meets the audit objectives defined below:

System and data are validated.

System meets all user requirements.

System meets all control requirements.

A. Programming and training

B. Evaluation and acceptance

C. Definition

D. Initiation

Answer: (SHOW ANSWER)

It is the evaluation and acceptance phase of the SDLC, which meets the following audit objectives:

System and data are validated.

System meets all user requirements.

System meets all control requirements

Answer option D is incorrect. During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

Answer option C is incorrect. During the definition phase, users' needs are defined and the needs are translated into requirements statements that incorporate appropriate controls. Answer option A is incorrect. During the programming and training phase, the software and other components of the system are faithfully incorporated into the design specifications. Proper documentation and training are provided in this phase.

Reference: CISM Review Manual 2010, Contents: "Information security process management"

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 152

Which of the following BEST describes why the "second line of defense" (risk/compliance function) should NOT perform the same duties as the "first line" (operational management)?

- A. There is no meaningful distinction between the lines
- B. Blending these roles undermines the independence needed for effective risk oversight and creates conflicts of interest
- C. The second line should always directly control the first line's daily operations
- D. The lines are interchangeable depending on organizational size

Answer: (SHOW ANSWER)

The value of the three lines of defense model relies on appropriate separation - if the risk/compliance function directly performs operational tasks, its ability to independently oversee and challenge those operations is compromised.

NEW QUESTION: 153

How many change control systems are there in project management?

- A. 2
- B. 4
- C. 3
- D. 1

Answer: (SHOW ANSWER)

NEW QUESTION: 154

Which of the following are the examples of administrative controls? Each correct answer represents a complete solution. Choose all that apply.

- A. Security awareness training
- B. Security policy
- C. Data Backup
- D. Auditing

Answer: A,B ([LEAVE A REPLY](#))

The following are the examples of administrative controls.

Security awareness training

Security policy

Personnel controls

Answer option C is incorrect. Data backup is an example of physical controls. Answer option D is incorrect. Auditing is an example of technical controls.

Reference: "http://en.wikipedia.org/wiki/Information_security#Administrative "

NEW QUESTION: 155

Which of the following persons is responsible for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not?

- A. Data custodian
- B. Auditor
- C. User
- D. Data owner

Answer: ([SHOW ANSWER](#)**)**

An auditor is liable for testing and verifying whether the security policy is properly implemented, and the derived security solutions are adequate or not. It is the responsibility of the auditor to generate the compliance and effectiveness reports, which are reviewed by the senior management. Answer option A is incorrect. The data custodian is responsible for the task of implementing the prescribed protection defined by the security policy and upper management.

Answer option D is incorrect. The data owner is responsible for classifying information for placement and protection within the security solution.

Answer option C is incorrect. The user can be any person who has access to the secured system.

Reference: Building an Information Security Awareness Program, Contents. "Working with the Auditors for Fun and Pleasure"

NEW QUESTION: 156

Which of the following is the correct order of digital investigations Standard Operating Procedure (SOP)?

- A. Initial analysis, request for service, data collection, data reporting, data analysis
- B. Initial analysis, request for service, data collection, data analysis, data reporting
- C. Request for service, initial analysis, data collection, data analysis, data reporting
- D. Request for service, initial analysis, data collection, data reporting, data analysis

Answer: ([SHOW ANSWER](#)**)**

A standard operating procedure is a set of instructions having the force of a directive, covering those features of operations that lend themselves to a definite or standardized procedure without loss of effectiveness. Standard Operating Policies and Procedures can be effective catalysts to drive performance improvement and improve organizational results. Every good quality system is based on its standard operating procedures (SOPs). Steps of standard operating procedures are as follows:

- 1.Request for service
- 2.Initial analysis
- 3.Data collection
- 4.Data analysis
- 5.Data reporting

Answer options B, D, and A are incorrect. All these are not the correct order of digital investigations Standard Operating Procedure (SOP).

Standard Operating Procedure (SOP) describes a best practice approach to executing tasks related to the production and maintenance of hardware and software, as well as incident and change management. There are a number of solutions available to automate the execution of SOPs for large enterprises, as it pertains to information technology, such as Creekside, iConclude and Stratavia.

Reference: CHFI Course Manual, Contents: "Computer Forensics"

NEW QUESTION: 157

Which of the following liabilities is a third-party liability in which an individual may be responsible for an action by another party?

- A. Engaged liability
- B. Vicarious liability
- C. Relational liability
- D. Contributory liability

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 158

Which of the following is a set of exclusive rights granted by a state to an inventor or his assignee for a fixed period of time in exchange for the disclosure of an invention?

- A. Snooping
- B. Patent
- C. Utility model
- D. Copyright

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 159

You work as the Network Administrator for a defense contractor. Your company works with sensitive materials and all IT personnel have at least a secret level clearance. You are still concerned that one individual could perhaps compromise the network (intentionally or unintentionally) by setting up improper or unauthorized remote access. What is the best way to avoid this problem?

- A. Implement separation of duties.
- B. Implement RBAC.
- C. Implement three way authentication.
- D. Implement least privileges.

Answer: A ([LEAVE A REPLY](#))

If no single employee has total control over a process (like setting up remote access) then no individual can compromise security. Having more than one person involved in any key processes by separating duties, will help prevent both intentional and unintentional security breaches.

Answer option D is incorrect. Least privileges simply mean each user has only those privileges needed to do their job tasks. Someone must have the authorization to create remote links, therefore, least privileges won't help.

Answer option C is incorrect. No method of authenticating users will address the issue of an authorized administrator creating a security breach.

Answer option B is incorrect. No method of access control will address the issue of an authorized administrator creating a security breach.

Reference: "http://www.networksasia.net/article.php?id_article=4318"

NEW QUESTION: 160

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software.

Which of the following SDLC phases meets the audit objectives defined below: System and data are validated. System meets all user requirements. System meets all control requirements.

A. Definition

B. Initiation

C. Programming and training

D. Evaluation and acceptance

Answer: **([SHOW ANSWER](#))**

NEW QUESTION: 161

Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. DITSCAP

B. ASSET

C. NSA-IAM

D. NIACAP

Answer: **D** ([LEAVE A REPLY](#))

NEW QUESTION: 162

Mark is the project manager of the NHQ project in Spartech Inc. The project has an asset valued at \$195,000 and is subjected to an exposure factor of 35 percent. What will be the Single Loss Expectancy of the project?

A. \$92,600

B. \$67,250

C. \$68,250

D. \$72,650

Answer: **C** ([LEAVE A REPLY](#))

The Single Loss Expectancy (SLE) of this project will be \$68,250. Single Loss Expectancy is a term related to Risk Management and Risk Assessment. It can be defined as the monetary value expected from the occurrence of a risk on an asset. It is mathematically expressed as follows.

Single Loss Expectancy (SLE) = Asset Value (AV) * Exposure Factor (EF) where the Exposure Factor is represented in the impact of the risk over the asset, or percentage of asset lost. As an example, if the Asset Value is reduced two thirds, the exposure factor value is .66. If the asset is completely lost, the Exposure Factor is 1.0. The result is a monetary value in the same unit as the Single Loss Expectancy is expressed.

Here, it is as follows.

$SLE = \text{Asset Value} * \text{Exposure Factor}$

$= 195,000 * 0.35$

$= \$68,250$

Answer options A, D, and B are incorrect. These are not valid SLE's for this project.

NEW QUESTION: 163

Which of the following characteristics are described by the DIAP Information Readiness Assessment function?

Each correct answer represents a complete solution. Choose all that apply.

- A.** It provides data needed to accurately assess IA readiness.
- B.** It identifies and generates IA requirements.
- C.** It performs vulnerability/threat analysis assessment.
- D.** It provides for entry and storage of individual system data.

Answer: A,B,C ([LEAVE A REPLY](#))

NEW QUESTION: 164

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement?

Each correct answer represents a complete solution. Choose all that apply.

- A.** Information dissemination policy
- B.** Electronic monitoring statement
- C.** Additional personnel security controls
- D.** Incident response plan

Answer: A,B,C,D ([LEAVE A REPLY](#))

When the incident response team has turned the evidence over to the forensic team, it starts looking for the ways to improve the incident response process. The typical areas for improvement are as follows.

Incident response plan

Information dissemination policy

Incident reporting policy

Electronic monitoring statement

Audit trail policy

Additional personnel security controls

Reference: CHFI Manuals, Contents. "Incident Response"

NEW QUESTION: 165

Which of the following BEST describes the concept of "security through the lifecycle" as emphasized in ISSMP?

- A.** Security is only relevant during the design phase
- B.** Security considerations are integrated from initiation through disposal of a system or project
- C.** Security is applied only after an incident occurs
- D.** Security is the sole responsibility of developers

Answer: B ([LEAVE A REPLY](#))

ISSMP promotes embedding security across the entire system/project lifecycle - planning, design, implementation, operations, and disposal - rather than treating it as an afterthought or one-time activity.

NEW QUESTION: 166

Which of the following issues are addressed by the change control phase in the maintenance phase of the life cycle models? Each correct answer represents a complete solution. Choose all that apply.

- A. Recreating and analyzing the problem
- B. Establishing the priorities of requests
- C. Developing the changes and corresponding tests
- D. Performing quality control

Answer: A,C,D ([LEAVE A REPLY](#))

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 167

Your project team has identified a project risk that must be responded to. The risk has been recorded in the risk register and the project team has been discussing potential risk responses for the risk event. The event is not likely to happen for several months but the probability of the event is high. Which one of the following is a valid response to the identified risk event?

- A. Corrective action
- B. Risk audit
- C. Technical performance measurement
- D. Earned value management

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 168

Which of the following is the default port for Simple Network Management Protocol (SNMP)?

- A. TCP port 80
- B. TCP port 25
- C. UDP port 161
- D. TCP port 110

Answer: C ([LEAVE A REPLY](#))

UDP port 161 is the default port for SNMP.

What is SNMP?

Simple Network Management Protocol (SNMP) is a part of the TCP/IP protocol suite, which allows users to manage the network. SNMP is used to keep track of what is being used on the network and how the object is behaving.

Answer option A is incorrect. TCP port 80 is the default port for Hypertext Transfer Protocol (HTTP). Answer option D is incorrect. TCP port 110 is the default port for Post Office Protocol version 3 (POP3).

Answer option B is incorrect. TCP port 25 is the default port for Simple Mail Transfer Protocol (SMTP).

Reference: TechNet, Contents. "Chapter 1 - Introduction to TCP/IP"

NEW QUESTION: 169

You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when conducting a security awareness campaign?

- A. Provide technical details on exploits.
- B. Provide customized messages for different groups.
- C. Target system administrators and the help desk.
- D. Target senior managers and business process owners.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 170

Which of the following BEST describes the concept of "dwell time" in the context of an advanced persistent threat (APT) compromise?

- A. The time it takes to patch a vulnerability after disclosure
- B. The length of time an attacker remains undetected within a compromised environment
- C. The duration of a penetration test engagement
- D. The time required to restore from backup

Answer: B ([LEAVE A REPLY](#))

Dwell time measures how long an intruder operates within a network before being detected - a key metric for evaluating detection capability maturity; shorter dwell time generally reduces potential damage.

NEW QUESTION: 171

Which of the following BEST describes the purpose of a "damage assessment" immediately following a disaster event?

- A. To calculate insurance premiums for the following year
- B. To evaluate the extent of impact on facilities, systems, and personnel to inform recovery decisions and prioritization
- C. Damage assessment is performed only after full recovery is complete
- D. Damage assessment is solely a legal function

Answer: B ([LEAVE A REPLY](#))

An initial damage assessment informs which recovery strategy (e.g., invoke DRP, activate alternate site) is appropriate and helps prioritize which systems/functions need immediate attention based on actual impact.

NEW QUESTION: 172

Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

- A. 18 U.S.C. 1362
- B. 18 U.S.C. 1030
- C. 18 U.S.C. 2510
- D. 18 U.S.C. 2701
- E. 18 U.S.C. 1029

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 173

Which of the following test methods has the objective to test the IT system from the viewpoint of a threat-source and to identify potential failures in the IT system protection schemes?

- A. Penetration testing
- B. Security Test and Evaluation (ST&E)
- C. On-site interviews
- D. Automated vulnerability scanning tool

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 174

Which of the following BEST describes a "single point of failure" in the context of business continuity?

- A. A redundant system with automatic failover
- B. A component whose failure would disrupt the entire system or process with no alternative
- C. A backup power generator
- D. A geographically distributed data center

Answer: B ([LEAVE A REPLY](#))

A single point of failure is a critical dependency lacking redundancy; its failure causes total disruption. BCP efforts specifically aim to identify and eliminate these.

NEW QUESTION: 175

Which of the following statements about system hardening are true? Each correct answer represents a complete solution. Choose two.

- A. It can be achieved by installing service packs and security updates on a regular basis.
- B. It is used for securing the computer hardware.
- C. It can be achieved by locking the computer room.
- D. It is used for securing an operating system.

Answer: A,D ([LEAVE A REPLY](#))

System hardening is a term used for securing an operating system. It can be achieved by installing the latest service packs, removing unused protocols and services, and limiting the number of users with administrative privileges.

Reference: TechNet, Contents: "Data Security and Data Availability in the Administrative Authority"

NEW QUESTION: 176

Mark works as a security manager for SoftTech Inc. He is performing a security awareness program. To be successful in performing the awareness program, he should take into account the needs and current levels of training and understanding of the employees and audience. There are five key ways, which Mark should keep in mind while performing this activity. Current level of computer usage What the audience really wants to learn How receptive the audience is to the security program How to gain acceptance Who might be a possible ally Which of the following activities is performed in this security awareness process?

- A. Stunned owl syndrome
- B. Separation of duties
- C. Audience participation

D. Audience segmentation

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 177

Fill in the blank with an appropriate phrase. _____ is the process of using a strategy and plan of what patches should be applied to which systems at a specified time.

Answer:

Patch management

Explanation:

Patch management is the process of using a strategy and plan of what patches should be applied to which systems at a specified time. It is the process included in the overall system management. The initiative behind building patch management is to identify and test various types of code changes, with an eye to make the programming code function with a greater degree of efficiency.

Patch management broadens itself to the actual implementation of the code changes and monitors the function of the code to identify any unforeseen circumstances that did not emerge during the testing phase.

NEW QUESTION: 178

Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

A. Post-it note

B. Internet teleconferencing

C. Instant messaging

D. Blogs

E. Internet telephony

F. Electronic mail

Answer: B,C,D,E,F ([LEAVE A REPLY](#))

NEW QUESTION: 179

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

A. Determining what level of classification the information requires

B. Running regular backups and routinely testing the validity of the backup data

C. Controlling access, adding and removing privileges for individual users

D. Performing data restoration from the backups when necessary

Answer: B,C,D ([LEAVE A REPLY](#))

The owner of information delegates the responsibility of protecting that information to a custodian.

The following are the responsibilities of a custodian with regard to data in an information classification program.

Running regular backups and routinely testing the validity of the backup data Performing data restoration from the backups when necessary Controlling access, adding and removing privileges for individual users Answer option A is incorrect. Determining what level of classification the information requires is the responsibility of the owner.

Reference: "http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci995767,00.html"

NEW QUESTION: 180

Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

- A. Contract
- B. Proposal
- C. Service level agreement
- D. Outsource

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 181

Which of the following divisions of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy?

- A. Division A
- B. Division D
- C. Division B
- D. Division C

Answer: C ([LEAVE A REPLY](#))

Division B of the Trusted Computer System Evaluation Criteria (TCSEC) is based on the Mandatory Access Control (MAC) policy.

Mandatory Access Control (MAC) is a model that uses a predefined set of access privileges for an object of the system. Access to an object is restricted on the basis of the sensitivity of the object and granted through authorization. Sensitivity of an object is defined by the label assigned to it. For example, if a user receives a copy of an object that is marked as "secret", he cannot grant permission to other users to see this object unless they have the appropriate permission.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 182

Which of the following BEST describes the concept of "asset criticality tiering" when planning DR strategies?

- A. All assets should receive identical recovery priority regardless of function
- B. Assets are categorized into tiers based on business importance, driving differentiated RTO/RPO targets and recovery investment
- C. Criticality tiering applies only to hardware, never applications
- D. Tiering eliminates the need for a BIA

Answer: B ([LEAVE A REPLY](#))

Not all systems warrant the same recovery investment; tiering (e.g., Tier 1 mission-critical vs. Tier

3 non-critical) allows organizations to allocate DR resources proportionally to business impact, derived from the BIA.

NEW QUESTION: 183

Which of the following BEST describes the purpose of "security orchestration, automation, and response (SOAR)" from a management perspective?

- A. To eliminate the need for a SOC team entirely
- B. To improve efficiency and consistency of incident response by automating repetitive tasks and orchestrating tools/workflows
- C. To replace the incident response plan
- D. To function solely as a marketing tool

Answer: B (LEAVE A REPLY)

SOAR platforms help SOC teams respond faster and more consistently by automating routine tasks (e.g., enrichment, containment actions) and coordinating across tools - augmenting, not replacing, human analysts.

NEW QUESTION: 184

Drag and drop the Response management plans to match up with their respective purposes.

Drag an item from the item list and drop it on the appropriate spot. To remove an item, drag and drop it anywhere on the window.

PURPOSE	PLAN
It provides measures for sustaining essential business operations while recovering from a significant disruption.	Drop Here
It provides measures for recovering business operations immediately following a disaster.	Drop Here
It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.	Drop Here
It provides measures and capabilities for recovering a major application or general support system.	Drop Here
It provides measures for disseminating status report to personnel and the public.	Drop Here
It provides detailed measures to facilitate recovery of capabilities at an alternate site.	Drop Here

Disaster recovery plan

Crisis communication plan

Contingency plan

Continuity of operation plan

Business recovery plan

Business continuity plan

Answer:

Drag an item from the item list and drop it on the appropriate spot. To remove an item, drag and drop it anywhere on the window.

PURPOSE	PLAN
It provides measures for sustaining essential business operations while recovering from a significant disruption.	Business continuity plan
It provides measures for recovering business operations immediately following a disaster.	Business recovery plan
It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.	Continuity of operation plan
It provides measures and capabilities for recovering a major application or general support system.	Contingency plan
It provides measures for disseminating status report to personnel and the public.	Crisis communication plan
It provides detailed measures to facilitate recovery of capabilities at an alternate site.	Disaster recovery plan

Explanation:

The response management plans are shown in the table below:

Business continuity plan It provides measures for sustaining essential business operations while recovering from a significant disruption.

Business recovery plan It provides measures for recovering business operations immediately following a disaster.

Continuity of operation plan It provides measures and capabilities to maintain organizational essential, strategic functions at an alternate site for upto 30 days.

Contingency plan It provides measures and capabilities for recovering a major application or general support system.

Crisis communication plan It provides measures for disseminating status report to personnel and the public.

Disaster recovery plan It provides detailed measures to facilitate recovery of capabilities at an alternate site.

Reference: CISM Review Manual 2010, Contents: "Incident management and response"

NEW QUESTION: 185

Which of the following BEST describes why "board-level risk reporting" should avoid excessive technical jargon?

- A. Boards are technically proficient and prefer jargon
- B. Board members need risk information translated into business terms (financial, reputational, operational impact) to make informed governance decisions
- C. Technical jargon improves board decision-making
- D. Board-level reporting is not a security management responsibility

Answer: B (LEAVE A REPLY)

Boards are accountable for organizational risk oversight but typically lack deep technical expertise; effective reporting translates technical risk into business impact language so the board can make informed strategic decisions.

NEW QUESTION: 186

Electronic communication technology refers to technology devices, such as computers and cell phones, used to facilitate communication. Which of the following is/are a type of electronic communication? Each correct answer represents a complete solution. Choose all that apply.

- A. Electronic mail
- B. Instant messaging
- C. Internet teleconferencing
- D. Post-it note
- E. Blogs
- F. Internet telephony

Answer: A,B,C,E,F ([LEAVE A REPLY](#))

NEW QUESTION: 187

Which of the following BEST describes why "encryption key management" is considered a critical governance issue, not just a technical one?

- A. Key management has no governance implications
- B. Poor key management (e.g., lost keys, inadequate access controls, no rotation policy) can undermine the value of encryption and create business continuity/access risk
- C. Encryption keys should never be rotated once created
- D. Key management is solely the responsibility of end users

Answer: B ([LEAVE A REPLY](#))

Beyond the technical mechanics, key management involves policy decisions on ownership, access, rotation, backup, and escrow - poor governance can lock the organization out of its own data or expose keys to misuse.

NEW QUESTION: 188

Which of the following statements best explains how encryption works on the Internet?

- A. Encryption validates a username and password before sending information to the Web server.
- B. Encryption encodes information using specific algorithms with a string of numbers known as a key.
- C. Encryption helps in transaction processing by e-commerce servers on the Internet.
- D. Encryption allows authorized users to access Web sites that offer online shopping.

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 189

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. Which of the following are some of its critical steps? Each correct answer represents a complete solution. Choose two.

- A. Awareness and Training Material Effectiveness
- B. Awareness and Training Material Development
- C. Awareness and Training Material Implementation
- D. Awareness and Training Program Design

Answer: B,D ([LEAVE A REPLY](#))

NIST Special Publication 800-50 is a security awareness program. It is designed for those people who are currently working in the information technology field and want information on security policies. It supports the requirements that are specified in the Federal Information Security Management Act (FISMA) of 2002 and the Office of Management and Budget (OMB) Circular A-130, Appendix III. In this program, people can learn security policies, procedures, and techniques that can help them secure their IT resources. The IT security awareness program identifies four critical steps, which are as follows.

Awareness and Training Program Design (Section 3). The training documents are developed and approved for the support of the security awareness program. Awareness and Training Material Development (Section 4). This step of the security awareness program focuses on the availability of training resources and material. Program Implementation (Section 5). This step focuses on the delivery of the training material and addresses effective communication and roll-out of the awareness and training program. Post-Implementation (Section 6). This step focuses on the effectiveness of the security awareness program.

NEW QUESTION: 190

Which of the following is the process performed between organizations that have unique hardware or software that cannot be maintained at a hot or warm site?

- A. Cold sites arrangement
- B. Duplicate processing facilities
- C. Reciprocal agreements
- D. Business impact analysis

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 191

Which of the following processes will you involve to perform the active analysis of the system for any potential vulnerabilities that may result from poor or improper system configuration, known and/or unknown hardware or software flaws, or operational weaknesses in process or technical countermeasures?

- A. Baselineing
- B. Penetration testing
- C. Risk analysis
- D. Compliance checking

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 192

Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

- A. Disaster recovery plan
- B. Contingency plan
- C. Continuity of Operations Plan
- D. Business continuity plan

Answer: B ([LEAVE A REPLY](#))

A contingency plan is a plan devised for a specific situation when things could go wrong.

Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption. Answer option C is incorrect. It includes the plans and procedures documented that ensure the continuity of critical operations during any period where normal operations are impossible. Answer option A is incorrect. Disaster recovery planning is a subset of a larger process known as business continuity planning and should include planning for resumption of applications, data, hardware, communications (such as networking), and other IT infrastructure. A business continuity plan (BCP) includes planning for non-IT related aspects such as key personnel, facilities, crisis communication, and reputation protection, and should refer to the disaster recovery plan (DRP) for IT-related infrastructure recovery/continuity. Answer option D is incorrect. Business continuity planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan. The BCP lifecycle is as follows:

NEW QUESTION: 193

Which of the following statements reflect the 'Code of Ethics Canons' in the '(ISC)2 Code of Ethics'?

Each correct answer represents a complete solution. Choose all that apply.

- A.** Provide diligent and competent service to principals.
- B.** Protect society, the commonwealth, and the infrastructure.
- C.** Give guidance for resolving good versus good and bad versus bad dilemmas.
- D.** Act honorably, honestly, justly, responsibly, and legally.

Answer: ([SHOW ANSWER](#))

The Code of Ethics Canons in (ISC)2 code of ethics are as follows:

Protect society, the commonwealth, and the infrastructure. Act honorably, honestly, justly, responsibly, and legally.

Provide diligent and competent service to principals.

Advance and protect the profession.

Reference: <https://www.isc2.org/ethics/default.aspx>

NEW QUESTION: 194

Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

- A.** They are considered an indicator of threats coupled with vulnerability.
- B.** They can be removed completely by taking proper actions.
- C.** They can be analyzed and measured by the risk analysis process.
- D.** They can be mitigated by reviewing and taking responsible actions based on possible risks.

Answer: **A,C,D** ([LEAVE A REPLY](#))

NEW QUESTION: 195

Which of the following protocols is used with a tunneling protocol to provide security?

- A.** FTP
- B.** IPX/SPX

C. IPSec

D. EAP

Answer: C ([LEAVE A REPLY](#))

Internet Protocol Security (IPSec) is used with Layer 2 Tunneling Protocol (L2TP). It is a standard-based protocol that provides the highest level of virtual private network (VPN) security.

IPSec can encrypt virtually everything above the networking layer. It secures both data and password.

NEW QUESTION: 196

What is a stakeholder analysis chart?

A. It is a matrix that identifies all of the stakeholders and to whom they must report to.

B. It is a matrix that documents stakeholders' threats, perceived threats, and communication needs.

C. It is a matrix that documents the stakeholders' requirements, when the requirements were created, and when the fulfillment of the requirements took place..

D. It is a matrix that identifies who must communicate with whom.

Answer: B ([LEAVE A REPLY](#))

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (**447** Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 197

Which of the following are the responsibilities of a custodian with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

A. Running regular backups and routinely testing the validity of the backup data

B. Determining what level of classification the information requires

C. Controlling access, adding and removing privileges for individual users

D. Performing data restoration from the backups when necessary

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 198

Which of the following BEST describes the purpose of a "war room" during a major incident?

A. A physical/virtual space for centralized coordination and decision-making during response

B. A location for storing backup tapes

C. A room dedicated to employee training

D. A secure facility for destroying evidence

Answer: A ([LEAVE A REPLY](#))

A war room centralizes communication and coordination among response teams and stakeholders during a significant incident, improving situational awareness and decision speed.

NEW QUESTION: 199

Which of the following statements best explains how encryption works on the Internet?

- A. Encryption helps in transaction processing by e-commerce servers on the Internet.
- B. Encryption allows authorized users to access Web sites that offer online shopping.
- C. Encryption validates a username and password before sending information to the Web server.
- D. Encryption encodes information using specific algorithms with a string of numbers known as a key.

Answer: D ([LEAVE A REPLY](#))

NEW QUESTION: 200

The incident response team has turned the evidence over to the forensic team. Now, it is the time to begin looking for the ways to improve the incident response process for next time. What are the typical areas for improvement? Each correct answer represents a complete solution. Choose all that apply.

- A. Information dissemination policy
- B. Electronic monitoring statement
- C. Additional personnel security controls
- D. Incident response plan

Answer: A,B,C,D ([LEAVE A REPLY](#))

Explanation/Reference:

NEW QUESTION: 201

Which of the following architecturally related vulnerabilities is a hardware or software mechanism, which was installed to permit system maintenance and to bypass the system's security protections?

- A. Maintenance hook
- B. Covert channel
- C. Lack of parameter checking
- D. Time of Check to Time of Use (TOC/TOU) attack

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 202

Which of the following BEST describes why "independence" is important for an internal audit function reviewing the security program?

- A. Independence is not necessary for internal audits
- B. Independence (e.g., reporting outside the security organization) ensures objective, unbiased evaluation of controls without conflict of interest
- C. Auditors should report directly to the CISO to ensure alignment
- D. Independence only matters for external auditors

Answer: B ([LEAVE A REPLY](#))

For audit findings to be credible and objective, the audit function typically reports independently (e.g., to an audit committee or board) rather than to the function it is reviewing, avoiding conflicts of interest.

NEW QUESTION: 203

Which of the following statements are true about a hot site? Each correct answer represents a complete solution. Choose all that apply.

- A.** It can be used within an hour for data recovery.
- B.** It is cheaper than a cold site but more expensive than a warm site.
- C.** It is the most inexpensive backup site.
- D.** It is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

Answer: A,D ([LEAVE A REPLY](#))

A hot site is a duplicate of the original site of the organization, with full computer systems as well as near-complete backups of user data.

A hot site can be used within an hour for data recovery.

The capacity of the hot site may or may not match the capacity of the original site depending on the organization's requirements. This type of backup site is the most expensive to operate. Hot sites are popular with organizations that operate real time processes such as financial institutions, government agencies, and ecommerce providers.

Answer options C and B are incorrect. A hot site is the most expensive site to operate since it contains all hardware as well as resources of the original site. A cold site is the most inexpensive type of backup site for an organization to operate since it does not include backed up copies of data and information from the original location of the organization, nor does it include hardware already set up. A warm site is, quite logically, a compromise between hot and cold in terms of resources and cost.

NEW QUESTION: 204

Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

- A.** Wiretapping
- B.** Data diddling
- C.** Eavesdropping
- D.** Spoofing

Answer: ([SHOW ANSWER](#)**)**

NEW QUESTION: 205

Which of the following BEST describes a "Computer Security Incident Response Team (CSIRT)" charter's PRIMARY purpose?

- A.** To document network diagrams
- B.** To formally define the CSIRT's mission, scope, authority, and responsibilities within the organization
- C.** To replace the need for an incident response plan
- D.** To list vendor contract terms

Answer: ([SHOW ANSWER](#)**)**

A CSIRT charter, approved by management, establishes the team's formal mandate - what it covers, what authority it has (e.g., to isolate systems), and how it relates to other business functions - providing legitimacy and clarity of role.

NEW QUESTION: 206

You are the project manager of the GHE Project. You have identified the following risks with the characteristics as shown in the following figure:

Risk	Probability	Impact
A	.60	-10,000
B	.10	-85,000
C	.25	-75,000
D	.40	45,000
E	.50	-17,000

How much capital should the project set aside for the risk contingency reserve?

- A. \$142,000
- B. \$232,000
- C. \$41,750
- D. \$23,750

Answer: D ([LEAVE A REPLY](#))

Contingency reserves are estimated costs to be used at the discretion of the project manager to deal with anticipated, but not certain, events. These events are "known unknowns" and are part of the project scope and cost baselines. The contingency reserve is calculated by multiplying the probability and the impact for the risk event value for each risk event. The sum of the risk events equals the contingency reserve for the project. Note that Risk D is a positive risk amount. Answer option C is incorrect. This value is the sum of the risk events if you did not include Risk D as a positive risk value.

NEW QUESTION: 207

Which of the following roles is typically responsible for developing and maintaining the organization's overall security awareness training program?

- A. Chief Financial Officer
- B. Security Awareness/Training Manager (often under CISO)
- C. External auditor
- D. Legal counsel

Answer: (SHOW ANSWER)

Security awareness and training is typically owned within the security organization, often reporting to the CISO, as part of the human risk management function.

NEW QUESTION: 208

Which of the following documents is described in the statement below? "It is developed along with all processes of the risk management. It contains the results of the qualitative risk analysis, quantitative risk analysis, and risk response planning."

- A. Risk register
- B. Project charter
- C. Risk management plan
- D. Quality management plan

Answer: A ([LEAVE A REPLY](#))

NEW QUESTION: 209

Which of the following BEST describes "security by design"?

- A. Adding security controls after a system is deployed
- B. Integrating security requirements and considerations into system architecture and design from the earliest stages
- C. A methodology used only for physical security
- D. A concept exclusive to hardware manufacturing

Answer: B ([LEAVE A REPLY](#))

Security by design embeds security into the architecture/design phase rather than retrofitting it later, reducing cost and improving effectiveness - closely related to "shift-left" and privacy by design principles.

NEW QUESTION: 210

Which of the following are the levels of public or commercial data classification system? Each correct answer represents a complete solution. Choose all that apply.

- A. Public
- B. Sensitive
- C. Private
- D. Secret
- E. Unclassified
- F. Confidential

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 211

Change Management is used to ensure that standardized methods and procedures are used for efficient handling of all changes. Who decides the category of a change?

- A. The Process Manager
- B. The Service Desk
- C. The Change Manager
- D. The Change Advisory Board
- E. The Problem Manager

Answer: C ([LEAVE A REPLY](#))

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount: **Exam-Tests**)

NEW QUESTION: 212

Eric is the project manager of the NQQ Project and has hired the ZAS Corporation to complete part of the project work for Eric's organization. Due to a change request the ZAS Corporation is no longer needed on the project even though they have completed nearly all of the project work. Is Eric's organization liable to pay the ZAS Corporation for the work they have completed so far on the project?

- A. Yes, the ZAS Corporation did not choose to terminate the contract work.
- B. It depends on what the outcome of a lawsuit will determine.
- C. It depends on what the termination clause of the contract stipulates.
- D. No, the ZAS Corporation did not complete all of the work.

Answer: ([SHOW ANSWER](#))

Explanation/Reference:

NEW QUESTION: 213

Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

- A. Delegating the responsibility of the data protection duties to a custodian.
- B. Running regular backups and routinely testing the validity of the backup data.
- C. Determining what level of classification the information requires.
- D. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.

Answer: A,C,D ([LEAVE A REPLY](#))

NEW QUESTION: 214

How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

- A. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)
- B. Exposure Factor (EF)/Single Loss Expectancy (SLE)
- C. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
- D. Asset Value X Exposure Factor (EF)

Answer: ([SHOW ANSWER](#))

NEW QUESTION: 215

Which of the following Acts enacted in United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

- A. Computer Fraud and Abuse Act
- B. Electronic Communications Privacy Act of 1986
- C. Wiretap Act
- D. Economic Espionage Act of 1996

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 216

Which of the following laws enacted in United States makes it illegal for an Internet Service Provider (ISP) to allow child pornography to exist on Web sites?

- A. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
- B. USA PATRIOT Act

- C. Sexual Predators Act
- D. Child Pornography Prevention Act (CPPA)

Answer: C ([LEAVE A REPLY](#))

NEW QUESTION: 217

Which of the following plans is documented and organized for emergency response, backup operations, and recovery maintained by an activity as part of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation?

- A. Disaster Recovery Plan
- B. Contingency Plan
- C. Continuity Of Operations Plan
- D. Business Continuity Plan

Answer: B ([LEAVE A REPLY](#))

Contingency plan is prepared and documented for emergency response, backup operations, and recovery maintained by an activity as the element of its security program that will ensure the availability of critical resources and facilitates the continuity of operations in an emergency situation. A contingency plan is a plan devised for a specific situation when things could go wrong. Contingency plans are often devised by governments or businesses who want to be prepared for anything that could happen. Contingency plans include specific strategies and actions to deal with specific variances to assumptions resulting in a particular problem, emergency, or state of affairs. They also include a monitoring process and "triggers" for initiating planned actions. They are required to help governments, businesses, or individuals to recover from serious incidents in the minimum time with minimum cost and disruption.

Answer option A is incorrect. A disaster recovery plan should contain data, hardware, and software that can be critical for a business. It should also include the plan for sudden loss such as hard disc crash. The business should use backup and data recovery utilities to limit the loss of data. Answer option C is incorrect. The Continuity Of Operation Plan (COOP) refers to the preparations and institutions maintained by the United States government, providing survival of federal government operations in the case of catastrophic events. It provides procedures and capabilities to sustain an organization's essential. COOP is the procedure documented to ensure persistent critical operations throughout any period where normal operations are unattainable.

Answer option D is incorrect. Business Continuity Planning (BCP) is the creation and validation of a practiced logistical plan for how an organization will recover and restore partially or completely interrupted critical (urgent) functions within a predetermined time after a disaster or extended disruption. The logistical plan is called a business continuity plan.

Reference: CISM Review Manual 2010, Contents. "Incident management and response"

NEW QUESTION: 218

Which of the following BEST describes the PRIMARY value of maintaining "offline/air-gapped backups" as part of a resilience strategy?

- A. Offline backups are unnecessary if cloud backups exist
- B. Physically or logically isolated backups provide a recovery option that is not reachable by network-based attacks like ransomware
- C. Air-gapped backups eliminate the need for RTO/RPO planning
- D. Offline backups should be tested only during an actual disaster

Answer: (SHOW ANSWER)

Because ransomware and other network-based attacks can spread to connected backup systems, maintaining truly isolated (air-gapped or offline) copies ensures a clean recovery source remains available even in a widespread compromise.

NEW QUESTION: 219

Which of the following BEST describes the purpose of a "risk register"?

- A. A list of all employees with security clearances
- B. A centralized document tracking identified risks, their analysis, owners, and treatment status
- C. A log of firewall rule changes
- D. A record of all completed security training

Answer: B ([LEAVE A REPLY](#))

The risk register is the primary tool for tracking identified risks throughout their lifecycle - description, likelihood, impact, owner, and treatment/mitigation status - used for ongoing monitoring and reporting.

NEW QUESTION: 220

Which of the following policies helps reduce the potential damage from the actions of one person?

- A. Internal audit
- B. Separation of duties
- C. Risk assessment
- D. CSA

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 221

Which of the following BEST describes the purpose of "breach simulation exercises" specifically involving executive leadership and legal/PR teams (distinct from technical IR drills)?

- A. To test firewall rule configurations
- B. To rehearse decision-making, regulatory notification timing, and public communication strategy under realistic pressure
- C. To replace technical incident response testing
- D. To satisfy insurance requirements only

Answer: (SHOW ANSWER)

Executive/legal/PR breach simulations focus on strategic and reputational dimensions - notification decisions, regulatory timelines, and public messaging - complementing (not replacing) technical response drills.

NEW QUESTION: 222

An organization is deciding between building an in-house SOC versus outsourcing to an MSSP.

Which factor is MOST relevant to this "make vs. buy" decision from an ISSMP management perspective?

- A. Preference of the CISO's personal working style
- B. Total cost of ownership, in-house expertise availability, and strategic control requirements
- C. The color scheme of the SOC dashboard
- D. The number of vendors currently in the market

Answer: B ([LEAVE A REPLY](#))

Make-vs-buy decisions should be grounded in business case analysis - cost, capability, control, and risk tradeoffs - reflecting ISSMP's business/management orientation rather than purely technical or personal preference.

NEW QUESTION: 223

Which of the following statements is true about auditing?

- A. It is used to protect the network against virus attacks.
- B. It is used to track user accounts for file and object access, logon attempts, etc.
- C. It is used to secure the network or the computers on the network.
- D. It is used to prevent unauthorized access to network resources.

Answer: B ([LEAVE A REPLY](#))

Auditing is used to track user accounts for file and object access, logon attempts, system shutdown etc. This enhances the security of the network. Before enabling auditing, the type of event to be audited should be specified in the Audit Policy in User Manager for Domains.

Answer option C is incorrect. Although auditing does help in enhancing the security of the network to some extent, it is not actually used for this purpose. Answer option A is incorrect. Anti-virus software prevents viruses from entering the network.

Reference: TechNet, Contents. "Chapter 10 - Implementing Security"

NEW QUESTION: 224

Which of the following BEST describes why a CISO should maintain relationships with peer organizations and information sharing groups (e.g., ISACs)?

- A. Information sharing is prohibited by law
- B. Collaborative threat intelligence sharing improves situational awareness and collective defense across the sector
- C. ISACs only serve government agencies
- D. Peer relationships have no value in incident response

Answer: B ([LEAVE A REPLY](#))

Information Sharing and Analysis Centers (ISACs) and similar groups allow organizations within a sector to share threat intelligence and best practices, improving early warning and collective resilience against common threats.

NEW QUESTION: 225

Software Development Life Cycle (SDLC) is a logical process used by programmers to develop software.

Which of the following SDLC phases meets the audit objectives defined below: System and data are validated.

System meets all user requirements. System meets all control requirements.

- A. Initiation
- B. Evaluation and acceptance
- C. Programming and training
- D. Definition

Answer: B ([LEAVE A REPLY](#))

NEW QUESTION: 226

Which of the following roles is responsible for formally accepting residual risk on behalf of the organization?

- A. Security analyst
- B. Risk owner / senior management
- C. Auditor
- D. Incident responder

Answer: B ([LEAVE A REPLY](#))

Residual risk acceptance is a business decision made by someone with the authority and accountability for the asset or process - typically senior management or a designated risk owner.

Answer options A, C, and D provide input or evaluation but lack the authority to formally accept risk.

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)

NEW QUESTION: 227

Which of the following BEST describes "attribution" in the context of threat intelligence, and a key challenge associated with it?

- A. Attribution is trivial and always certain
- B. Attribution is the process of identifying the source of an attack, which is often difficult and can be deliberately obscured by adversaries
- C. Attribution only matters for insider threats
- D. Attribution is irrelevant to incident response

Answer: B (LEAVE A REPLY)

Attribution - determining who is responsible for an attack - is notoriously difficult due to techniques like IP spoofing, false flags, and use of intermediary infrastructure, and often carries legal/political implications.

NEW QUESTION: 228

Which of the following analysis provides a foundation for measuring investment of time, money and human resources required to achieve a particular outcome?

- A. Requirement analysis
- B. Vulnerability analysis
- C. Cost-benefit analysis
- D. Gap analysis

Answer: (SHOW ANSWER)

Valid CISSP-ISSMP Dumps shared by TrainingDump.com for Helping Passing CISSP-ISSMP Exam! TrainingDump.com now offer the **newest CISSP-ISSMP exam dumps**, the TrainingDump.com CISSP-ISSMP exam **questions have been updated** and **answers have been corrected** get the **newest** TrainingDump.com CISSP-ISSMP dumps with Test Engine here:

<https://www.trainingdump.com/ISC/CISSP-ISSMP-practice-exam-dumps.html> (447 Q&As Dumps, **40%OFF** Special Discount:

Exam-Tests)