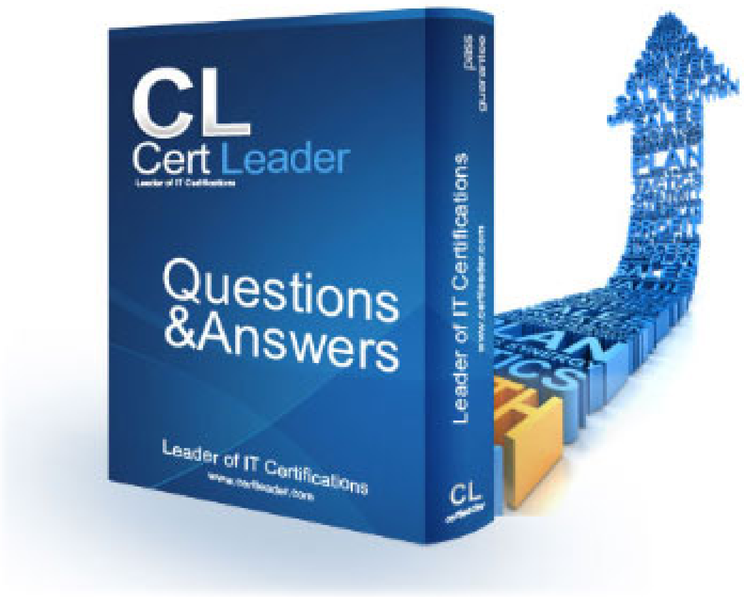
CISSP-ISSMP Dumps

Information Systems Security Management Professional

https://www.certleader.com/CISSP-ISSMP-dumps.html



NEW QUESTION 1
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. Configuration management
B. Risk management
C. Procurement management
D. Change management

Answer: A

NEW QUESTION 2
Which of the following are the ways of sending secure e-mail messages over the Internet? Each correct answer represents a complete solution. Choose two.

A. TLS
B. PGP
C. S/MIME
D. IPSec

Answer: BC

NEW QUESTION 3
Which of the following penetration testing phases involves reconnaissance or data gathering?

A. Attack phase
B. Pre-attack phase
C. Post-attack phase
D. Out-attack phase

Answer: B

NEW QUESTION 4
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. Business continuity plan
B. Disaster recovery plan
C. Continuity of Operations Plan
D. Contingency plan

Answer: D

NEW QUESTION 5
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

NEW QUESTION 6
Which of the following subphases are defined in the maintenance phase of the life cycle models?

A. Change control
B. Configuration control
C. Request control
D. Release control

Answer: ACD

NEW QUESTION 7
Which of the following terms refers to a mechanism which proves that the sender really sent a particular message?

A. Non-repudiation
B. Confidentiality
C. Authentication
D. Integrity

Answer: A

NEW QUESTION 8

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

Answer: ABC

NEW QUESTION 9
Joseph works as a Software Developer for Web Tech Inc. He wants to protect the algorithms and the techniques of programming that he uses in developing an application. Which of the following laws are used to protect a part of software?

A. Code Security law
B. Trademark laws
C. Copyright laws
D. Patent laws

Answer: D

NEW QUESTION 10
Which of the following is the best method to stop vulnerability attacks on a Web server?

A. Using strong passwords
B. Configuring a firewall
C. Implementing the latest virus scanner
D. Installing service packs and updates

Answer: D

NEW QUESTION 10
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

NEW QUESTION 11
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

NEW QUESTION 14
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: D

NEW QUESTION 18
Which of the following laws is the first to implement penalties for the creator of viruses, worms, and other types of malicious code that causes harm to the computer systems?

A. Gramm-Leach-Bliley Act
B. Computer Fraud and Abuse Act
C. Computer Security Act
D. Digital Millennium Copyright Act

Answer: B

NEW QUESTION 22
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 syste

Answer: AD

NEW QUESTION 25
Walter is the project manager of a large construction project. He'll be working with several vendors on the project. Vendors will be providing materials and labor for several parts of the project. Some of the works in the project are very dangerous so Walter has implemented safety requirements for all of the vendors and his own project team. Stakeholders for the project have added new requirements, which have caused new risks in the project. A vendor has identified a new risk that could affect the project if it comes into fruition. Walter agrees with the vendor and has updated the risk register and created potential risk responses to mitigate the risk. What should Walter also update in this scenario considering the risk event?

A. Project contractual relationship with the vendor
B. Project management plan
C. Project communications plan
D. Project scope statement

Answer: B

NEW QUESTION 29
Which of the following security controls will you use for the deployment phase of the SDLC to build secure software? Each correct answer represents a complete solution. Choose all that apply.

A. Vulnerability Assessment and Penetration Testing
B. Security Certification and Accreditation (C&A)
C. Change and Configuration Control
D. Risk Adjustments

Answer: ABD

NEW QUESTION 34
Which of the following can be prevented by an organization using job rotation and separation of duties policies?

A. Collusion
B. Eavesdropping
C. Buffer overflow
D. Phishing

Answer: A

NEW QUESTION 35
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. Names of the victims
B. Location of each incident
C. Nature of harassment
D. Date and time of incident

Answer: ABD

NEW QUESTION 39
Which of the following types of evidence is considered as the best evidence?

A. A copy of the original document
B. Information gathered through the witness's senses
C. The original document
D. A computer-generated record

Answer: C

NEW QUESTION 43
What are the purposes of audit records on an information system? Each correct answer represents a complete solution. Choose two.

A. Troubleshooting
B. Investigation
C. Upgradation
D. Backup

Answer: AB

NEW QUESTION 45

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

NEW QUESTION 46
A contract cannot have provisions for which one of the following?

A. Subcontracting the work
B. Penalties and fines for disclosure of intellectual rights
C. A deadline for the completion of the work
D. Illegal activities

Answer: D

NEW QUESTION 50
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

NEW QUESTION 54
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. One of the employees of your organization asks you the purpose of the security awareness, training and education program. What will be your answer?

A. It improves the possibility for career advancement of the IT staff.
B. It improves the security of vendor relations.
C. It improves the performance of a company's intranet.
D. It improves awareness of the need to protect system resource

Answer: D

NEW QUESTION 55
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: D

NEW QUESTION 58
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. Internet telephony
B. Instant messaging
C. Electronic mail
D. Post-it note
E. Blogs
F. Internet teleconferencing

Answer: ABCEF

NEW QUESTION 61
Which of the following acts is a specialized privacy bill that affects any educational institution to accept any form of funding from the federal government?

A. HIPAA
B. COPPA
C. FERPA
D. GLBA

Answer: C

NEW QUESTION 62
Which of the following steps is the initial step in developing an information security strategy?

A. Perform a technical vulnerabilities assessment.
B. Assess the current levels of security awareness.
C. Perform a business impact analysis.
D. Analyze the current business strateg

Answer: D

NEW QUESTION 65
Which of the following statements about the integrity concept of information security management are true? Each correct answer represents a complete solution. Choose three.

A. It ensures that unauthorized modifications are not made to data by authorized personnel orprocesses.
B. It determines the actions and behaviors of a single individual within a system
C. It ensures that modifications are not made to data by unauthorized personnel or processes.
D. It ensures that internal information is consistent among all subentities and also consistent with the real-world, external situation.

Answer: ACD

NEW QUESTION 69
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

NEW QUESTION 74
Ned is the program manager for his organization and he's considering some new materials for his program. He and his team have never worked with these materials before and he wants to ask the vendor for some additional information, a demon, and even some samples. What type of a document should Ned send to the vendor?

A. IFB
B. RFQ
C. RFP
D. RFI

Answer: D

NEW QUESTION 78
Against which of the following does SSH provide protection? Each correct answer represents a complete solution. Choose two.

A. IP spoofing
B. Broadcast storm
C. Password sniffing
D. DoS attack

Answer: AC

NEW QUESTION 83
What is a stakeholder analysis chart?

A. It is a matrix that documents stakeholders' threats, perceived threats, and communication needs.
B. It is a matrix that identifies all of the stakeholders and to whom they must report to.
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 who

Answer: A

NEW QUESTION 84
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. Disaster Recovery Plan
B. Continuity of Operations Plan
C. Contingency Plan
D. Business Continuity Plan

Answer: D

NEW QUESTION 86
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

NEW QUESTION 89
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: B

NEW QUESTION 93
Which of the following laws or acts, formed in Australia, enforces prohibition against cyber stalking?

A. Malicious Communications Act (1998)
B. Anti-Cyber-Stalking law (1999)
C. Stalking Amendment Act(1999)
D. Stalking by Electronic Communications Act (2001)

Answer: C

NEW QUESTION 98
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. CSIRT
B. CERT
C. FIRST
D. FedCIRC

Answer: C

NEW QUESTION 102
Which of the following statements is related with the first law of OPSEC?

A. If you are not protecting it (the critical and sensitive information), the adversary wins!
B. If you don't know what to protect, how do you know you are protecting it?
C. If you don't know about your security resources you could not protect your network.
D. If you don't know the threat, how do you know what toprotect?

Answer: D

NEW QUESTION 107
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 Problem Manager
B. The Process Manager
C. The Change Manager
D. The Service Desk
E. The Change Advisory Board

Answer: C

NEW QUESTION 110
Which of the following Acts enacted in United States amends Civil Rights Act of 1964, providing technical changes affecting the length of time allowed to challenge unlawful seniority provisions, to sue the federal government for discrimination and to bring age discrimination claims?

A. PROTECT Act
B. Sexual Predators Act
C. Civil Rights Act of 1991
D. The USA Patriot Act of 2001

Answer: C

NEW QUESTION 112
Which of the following policies helps reduce the potential damage from the actions of one person?

A. CSA
B. Risk assessment
C. Separation of duties
D. Internal audit

Answer: C

NEW QUESTION 115
The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes. Which of the following are Change Management terminologies? Each correct answer represents a part of the solution. Choose three.

A. Request for Change
B. Service Request Management
C. Change
D. Forward Schedule of Changes

Answer: ACD

NEW QUESTION 119
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: C

NEW QUESTION 123
James works as a security manager for SoftTech Inc. He has been working on the continuous process improvement and on the ordinal scale for measuring the maturity of the organization involved in the software processes. According to James, which of the following maturity levels of software CMM focuses on the continuous process improvement?

A. Repeatable level
B. Defined level
C. Initiating level
D. Optimizing level

Answer: D

NEW QUESTION 128
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. Patent
B. Utility model
C. Snooping
D. Copyright

Answer: A

NEW QUESTION 130
You are advising a school district on disaster recovery plans. In case a disaster affects the main IT centers for the district they will need to be able to work from an alternate location. However, budget is an issue. Which of the following is most appropriate for this client?

A. Cold site
B. Off site
C. Hot site
D. Warm site

Answer: A

NEW QUESTION 135
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. Warm site
C. Cold site
D. Hot site

Answer: B

NEW QUESTION 140
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. Scope changecontrol system
D. Project integration management

Answer: A

NEW QUESTION 142
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: CD

NEW QUESTION 146
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 legall

Answer: ABD

NEW QUESTION 149
Which of the following statements about Due Care policy is true?

A. It is a method used to authenticate users on a network.
B. It is a method for securing database servers.
C. It identifies the level of confidentiality of information.
D. It provides information about new viruse

Answer: C

NEW QUESTION 152
Part of your change management plan details what should happen in the change control system for your project. Theresa, a junior project manager, asks what the configuration management activities are for scope changes. You tell her that all of the following are valid configuration management activities except for which one?

A. Configuration Verification and Auditing
B. Configuration Item Costing
C. Configuration Identification
D. Configuration Status Accounting

Answer: B

NEW QUESTION 153
Which of the following is a documentation of guidelines that are used to create archival copies of important data?

A. User policy
B. Security policy
C. Audit policy
D. Backup policy

Answer: D

NEW QUESTION 154
Which of the following deals is a binding agreement between two or more persons that is enforceable by law?

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

Answer: C

NEW QUESTION 157
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

NEW QUESTION 162
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

NEW QUESTION 166
Which of the following sections come under the ISO/IEC 27002 standard?

A. Financial assessment
B. Asset management
C. Security policy
D. Risk assessment

Answer: BCD

NEW QUESTION 170
Which of the following U.S. Federal laws addresses computer crime activities in communication lines, stations, or systems?

A. 18 U.S.
B. 1362
C. 18 U.S.
D. 1030
E. 18 U.S.
F. 1029
G. 18 U.S.
H. 2701
I. 18 U.S.
J. 2510

Answer: A

NEW QUESTION 175
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

NEW QUESTION 177
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

NEW QUESTION 181
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. Penetration testing
B. Risk analysis
C. Baselining
D. Compliance checking

Answer: A

NEW QUESTION 185
Which of the following tools works by using standard set of MS-DOS commands and can create an MD5 hash of an entire drive, partition, or selected files?

A. Device Seizure
B. Ontrack
C. DriveSpy
D. Forensic Sorter

Answer: C

NEW QUESTION 190
Which of the following needs to be documented to preserve evidences for presentation in court?

A. Separation of duties
B. Account lockout policy
C. Incident response policy
D. Chain of custody

Answer: D

NEW QUESTION 191
Which of the following statutes is enacted in the U.S., which prohibits creditors from collecting data from applicants, such as national origin, caste, religion etc?

A. The Fair Credit Reporting Act (FCRA)
B. The Privacy Act
C. The Electronic Communications Privacy Act
D. The Equal Credit Opportunity Act (ECOA)

Answer: D

NEW QUESTION 192
Which of the following security models deal only with integrity? Each correct answer represents a complete solution. Choose two.

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

Answer: BD

NEW QUESTION 193
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

NEW QUESTION 197
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

NEW QUESTION 198
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

NEW QUESTION 201
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.

A. Configuration status accounting

Answer: A

NEW QUESTION 203
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.
Correct

A. Patch management

Answer: A

NEW QUESTION 204
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 dependson what the termination clause of the contract stipulates.
D. No, the ZAS Corporation did not complete all of the wor

Answer: C

NEW QUESTION 205
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: ACD

NEW QUESTION 210
You are working as a project manager in your organization. You are nearing the final stages of project execution and looking towards the final risk monitoring and controlling activities. For your project archives, which one of the following is an output of risk monitoring and control?

A. Quantitative risk analysis
B. Qualitative risk analysis
C. Requested changes
D. Risk audits

Answer: C

NEW QUESTION 213
Della works as a security manager for SoftTech Inc. She is training some of the newly recruited personnel in the field of security management. She is giving a tutorial on DRP. She explains that the major goal of a disaster recovery plan is to provide an organized way to make decisions if a disruptive event occurs and asks for the other objectives of the DRP. If you are among some of the newly recruited personnel in SoftTech Inc, what will be your answer for her question? Each correct answer represents a part of the solution. Choose three.

A. Protect an organization from major computer services failure.
B. Minimizethe risk to the organization from delays in providing services.
C. Guarantee the reliability of standby systems through testing and simulation.
D. Maximize the decision-making required by personnel during a disaste

Answer: ABC

NEW QUESTION 217
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: B

NEW QUESTION 222
Which of the following security issues does the Bell-La Padula model focus on?

A. Authentication
B. Confidentiality
C. Integrity
D. Authorization

Answer: B

NEW QUESTION 225
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: AB

NEW QUESTION 227
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. Child Pornography Prevention Act (CPPA)
B. USA PATRIOT Act
C. Prosecutorial Remedies and Tools Against the Exploitation of Children Today Act (PROTECT Act)
D. Sexual Predators Act

Answer: D

NEW QUESTION 230
Which of the following representatives of incident response team takes forensic backups of the systems that are the focus of the incident?

A. Legalrepresentative
B. Technical representative
C. Lead investigator
D. Information security representative

Answer: B

NEW QUESTION 234
You work as a Web Administrator for Perfect World Inc. The company is planning to host an E-commerce Web site. You are required to design a security plan for it. Client computers with different operating systems will access the Web server. How will you configure the Web server so that it is secure and only authenticated users are able to access it? Each correct answer represents a part of the solution. Choose two.

A. Use encrypted authentication.
B. Use the SSL protocol.
C. Use the EAP protocol.
D. Use Basic authenticatio

Answer: AB

NEW QUESTION 236
Which of the following statements are true about security risks? Each correct answer represents a complete solution. Choose three.

A. They can be analyzed and measured by the risk analysis process.
B. They can be removed completely by taking proper actions.
C. They can be mitigated by reviewing and taking responsible actions based on possible risks.
D. They are considered an indicator of threats coupled with vulnerabilit

Answer: ACD

NEW QUESTION 237
Which of the following methods for identifying appropriate BIA interviewees' includes examining the organizational chart of the enterprise to understand the functional positions?

A. Organizational chart reviews
B. Executive management interviews
C. Overlaying system technology
D. Organizational process models

Answer: A

NEW QUESTION 241
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. Lack of parameter checking
C. Time of Check to Time of Use (TOC/TOU) attack
D. Covert channel

Answer: A

NEW QUESTION 243
You have created a team of HR Managers and Project Managers for Blue Well Inc. The team will concentrate on hiring some new employees for the company and improving the organization's overall security by turning employees among numerous job positions. Which of the following steps will you perform to accomplish the task?

A. Job rotation
B. Job responsibility
C. Screening candidates
D. Separation of duties

Answer: A

NEW QUESTION 246
Your project has several risks that may cause serious financial impact should they happen. You have studied the risk events and made some potential risk responses for the risk events but
management wants you to do more. They'd like for you to create some type of a chart that identified the risk
probability and impact with a financial amount for each risk event. What is the likely outcome of creating this type of chart?

A. Quantitative analysis
B. Contingency reserve
C. Risk response
D. Risk response plan

Answer: B

NEW QUESTION 248
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: B

NEW QUESTION 253
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. Display of associated vulnerability components
C. Assessment of Risk
D. Identification of Critical Information

Answer: ACD

NEW QUESTION 256
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. Determining what level of classification the information requires.
B. Delegating the responsibility of the data protection duties to a custodian.
C. Reviewing the classification assignments at regular time intervals and making changes as the business needs change.
D. Running regular backups and routinely testing the validity of the backup dat

Answer: ABC

NEW QUESTION 260
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 privilege

Answer: A

NEW QUESTION 265

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

NEW QUESTION 270
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. Threaten to sue the vendor if they don't complete the work.
B. Fire the vendor for failing to complete the contractual obligation.
C. Withhold the vendor's payments for the work they've completed.
D. Refer to the contract agreement for directio

Answer: D

NEW QUESTION 274
How many change control systems are there in project management?

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

Answer: B

NEW QUESTION 277
In which of the following phases of the SDLC does the software and other components of the system faithfully incorporate the design specifications and provide proper documentation and training?

A. Programming andtraining
B. Evaluation and acceptance
C. Initiation
D. Design

Answer: A

NEW QUESTION 281
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: AD

NEW QUESTION 285
How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

A. Single Loss Expectancy (SLE)/ Exposure Factor (EF)
B. Asset Value X Exposure Factor (EF)
C. Exposure Factor (EF)/Single Loss Expectancy (SLE)
D. Single Loss Expectancy (SLE) X Annualized Rate of Occurrence (ARO)

Answer: D

NEW QUESTION 286
Which of the following rate systems of the Orange book has no security controls?

A. D-rated
B. C-rated
C. E-rated
D. A-rated

Answer: A

NEW QUESTION 288
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. Risk management plan
C. Quality management plan
D. Project charter

Answer: A

NEW QUESTION 289
Which of the following authentication protocols provides support for a wide range of authentication methods, such as smart cards and certificates?

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

Answer: B

NEW QUESTION 293
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. On-site interviews
C. Security Test and Evaluation (ST&E)
D. Automated vulnerability scanning tool

Answer: A

NEW QUESTION 295
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

NEW QUESTION 300
You are the project manager for TTX project. You have to procure some electronics gadgets for the project. A relative of yours is in the retail business of those gadgets. He approaches you for your favor to get the order. This is the situation of .

A. Conflict of interest
B. Bribery
C. Illegal practice
D. Irresponsible practice

Answer: A

NEW QUESTION 302
Which of the following is generally practiced by the police or any other recognized governmental authority?

A. Phishing
B. Wiretapping
C. SMB signing
D. Spoofing

Answer: B

NEW QUESTION 306
Which of the following is a documentation of guidelines that computer forensics experts use to handle evidences?

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

Answer: C

NEW QUESTION 311
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

NEW QUESTION 315
Which of the following statements is related with the second law of OPSEC?

A. If you are not protecting it (the critical and sensitive information), the adversary wins!
B. If you don't know what to protect, how do you know you are protecting it?
C. If you don't know about your security resources you could not protect your network.
D. If you don't know the threat, how do you know what to protect?

Answer: B

NEW QUESTION 318
Which of the following elements of BCP process includes the areas of plan implementation, plan testing, and ongoing plan maintenance, and also involves defining and documenting the continuity strategy?

A. Business continuity plan development
B. Business impact assessment
C. Scope and plan initiation
D. Plan approval and implementation

Answer: A

NEW QUESTION 319
Fill in the blank with an appropriate phrase. An is an intensive application of the OPSEC process to an existing operation or activity by a multidiscipline team of experts.

A. OPSEC assessment

Answer: A

NEW QUESTION 323
You work as a Product manager for Marioiss Inc. You have been tasked to start a project for securing the network of your company. You want to employ configuration management to efficiently manage the procedures of the project. What will be the benefits of employing configuration management for completing this project? Each correct answer represents a complete solution. Choose all that apply.

A. It provides object, orient, decide and act strategy.
B. It provides a live documentation of the project.
C. It provides the risk analysis of project configurations.
D. It provides the versions for network device

Answer: BD

NEW QUESTION 325
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. Secret
B. Sensitive
C. Unclassified
D. Private
E. Confidential
F. Public

Answer: BDEF

NEW QUESTION 330
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

NEW QUESTION 334
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

NEW QUESTION 338
Which of the following attacks can be mitigated by providing proper training to the employees in an organization?

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

Answer: A

NEW QUESTION 342
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. Preparea chain of custody and handle the evidence carefully.
B. Examine original evidence and never rely on the duplicate evidence.
C. Never exceed the knowledge base of the forensic investigation.
D. Follow the rules of evidence and never temper with the evidence.

Answer: ABCD

NEW QUESTION 343
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: BCD

NEW QUESTION 345
Which of the following statements about Hypertext Transfer Protocol Secure (HTTPS) are true? Each correct answer represents a complete solution. Choose two.

A. It uses TCP port 80 as the default port.
B. It is a protocol used in the Universal Resource Locater (URL) address line to connect to a secure site.
C. It uses TCP port 443 as the default port.
D. It is a protocol used to provide security for a database server in an internal networ

Answer: BC

NEW QUESTION 348
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 worm 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: AD

NEW QUESTION 351
You are the program manager for your project. You are working with the project managers regarding the procurement processes for their projects. You have ruled out one particular contract type because it is considered too risky for the program. Which one of the following contract types is usually considered to be the most dangerous for the buyer?

A. Cost plus incentive fee
B. Fixed fee
C. Cost plus percentage of costs
D. Time and materials

Answer: C

NEW QUESTION 354
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: B

NEW QUESTION 357
Which of the following plans provides procedures for recovering business operations immediately following a disaster?

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

Answer: D

NEW QUESTION 361
In which of the following contract types, the seller is reimbursed for all allowable costs for performing the contract work and receives a fixed fee payment which is calculated as a percentage of the initial estimated project costs?

A. Firm Fixed Price Contracts
B. Cost Plus Fixed Fee Contracts
C. Fixed Price Incentive Fee Contracts
D. Cost Plus Incentive Fee Contracts

Answer: B

NEW QUESTION 364
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

NEW QUESTION 365
Which of the following is the default port for Secure Shell (SSH)?

A. UDP port 161
B. TCP port 22
C. UDP port 138
D. TCP port 443

Answer: B

NEW QUESTION 368
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: ACD

NEW QUESTION 371
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: ACDE

NEW QUESTION 375
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: ABC

NEW QUESTION 380
Which of the following SDLC phases consists of the given security controls. Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

A. Design
B. Maintenance
C. Deployment
D. Requirements Gathering

Answer: A

NEW QUESTION 385
Which of the following liabilities is a third-party liability in which an individual may be responsible for an action by another party?

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

Answer: D

NEW QUESTION 387
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 managemen

Answer: B

NEW QUESTION 389
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

NEW QUESTION 391
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

NEW QUESTION 396
Which of the following sites are similar to the hot site facilities, with the exception that they are completely dedicated, self-developed recovery facilities?

A. Cold sites
B. Orange sites
C. Warm sites
D. Duplicate processing facilities

Answer: D

NEW QUESTION 400
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. Customary
B. Tort
C. Criminal
D. Administrative

Answer: A

NEW QUESTION 403
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 Imitative (IINI)

Answer: B

NEW QUESTION 408
You work as the project manager for Bluewell Inc. You are working on NGQQ Project for your company. You have completed the risk analysis processes for the risk events. You and the project team have created risk responses for most of the identified project risks. Which of the following risk response planning techniques will you use to shift the impact of a threat to a third party, together with the responses?

A. Risk mitigation
B. Risk acceptance
C. Risk avoidance
D. Risk transference

Answer: D

NEW QUESTION 412
In which of the following alternative processing sites is the backup facility maintained in a constant order, with a full complement of servers, workstations, and communication links ready to assume the primary operations responsibility?

A. Mobile Site
B. Cold Site
C. Warm Site
D. Hot Site

Answer: D

NEW QUESTION 413
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

NEW QUESTION 415
An organization monitors the hard disks of its employees' computers from time to time. Which policy does this pertain to?

A. Network security policy
B. Backup policy
C. Privacy policy
D. User password policy

Answer: C

NEW QUESTION 419
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

NEW QUESTION 423
Which of the following models uses a directed graph to specify the rights that a subject can transfer to an object or that a subject can take from another subject?

A. Take-Grant Protection Model
B. Bell-LaPadula Model
C. Biba Integrity Model
D. Access Matrix

Answer: A

NEW QUESTION 428
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. Businesscontinuity plan
B. Crisis communication plan
C. Contingency plan
D. Disaster recovery plan

Answer: A

NEW QUESTION 432
You work as the Senior Project manager in Dotcoiss Inc. Your company has started a software project using configuration management and has completed 70% of it. You need to ensure that the network infrastructure devices and networking standards used in this project are installed in accordance with the requirements of its detailed project design documentation. Which of the following procedures will you employ to accomplish the task?

A. Configuration identification
B. Physical configuration audit
C. Configuration control
D. Functional configuration audit

Answer: B

NEW QUESTION 435
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

NEW QUESTION 438
......