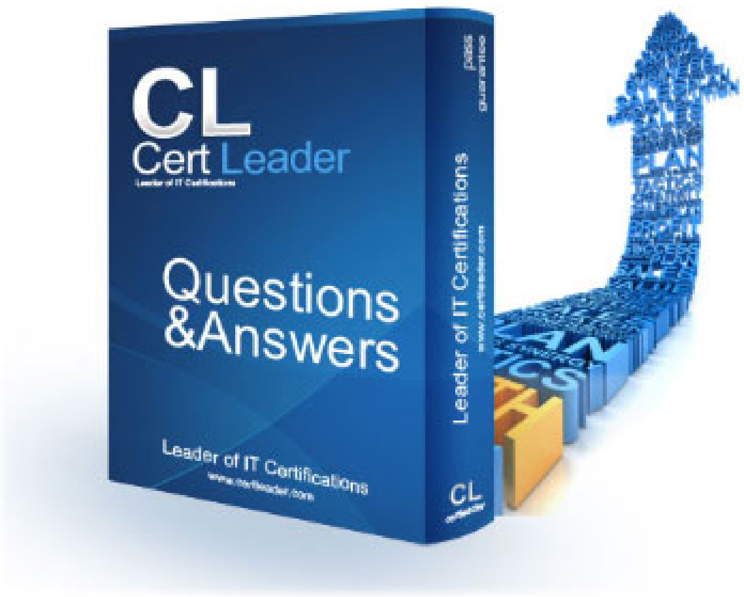
CISSP-ISSMP Dumps

Information Systems Security Management Professional

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



NEW QUESTION 1
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 2
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. Business impact analysis
C. Duplicate processing facilities
D. Reciprocal agreements

Answer: D

NEW QUESTION 3
Which of the following involves changing data prior to or during input to a computer in an effort to commit fraud?

A. Data diddling
B. Wiretapping
C. Eavesdropping
D. Spoofing

Answer: A

NEW QUESTION 4
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 5
Mark works as a security manager for SoftTech Inc. He is involved in the BIA phase to create a document to be used to help understand what impact a disruptive event would have on the business. The impact might be financial or operational. Which of the following are the objectives related to the above phase in which Mark is involved? Each correct answer represents a part of the solution. Choose three.

A. Resource requirements identification
B. Criticality prioritization
C. Down-time estimation
D. Performing vulnerability assessment

Answer: ABC

NEW QUESTION 6
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 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 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 9
Which of the following is NOT a valid maturity level of the Software Capability Maturity Model (CMM)?

A. Managed level
B. Defined level
C. Fundamental level
D. Repeatable level

Answer: C

NEW QUESTION 10
Which of the following BCP teams is the first responder and deals with the immediate effects of the disaster?

A. Emergency-management team
B. Damage-assessment team
C. Off-site storage team
D. Emergency action team

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 13
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. File and object access
C. Network logons and logoffs
D. Printer access

Answer: BCD

NEW QUESTION 16
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

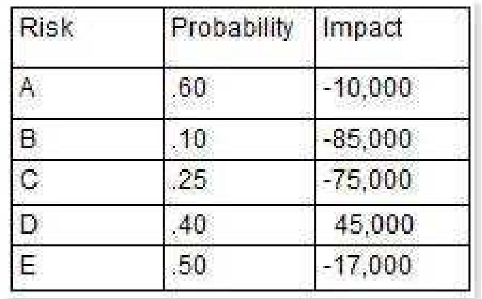
Answer: D

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 23
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

NEW QUESTION 26
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 28
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. Editor
B. Custodian
C. Owner
D. Security auditor
E. User

Answer: BCDE

NEW QUESTION 31
Which of the following processes is described in the statement below? "It is the process of implementing risk response plans, tracking identified risks, monitoring residual risk, identifying new risks, and evaluating risk process effectiveness throughout the project."

A. Monitor and Control Risks
B. Identify Risks
C. Perform Qualitative Risk Analysis
D. Perform Quantitative Risk Analysis

Answer: A

NEW QUESTION 33
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 37
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

NEW QUESTION 40
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 43
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 45
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 47
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 49
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. Requirementanalysis

Answer: C

NEW QUESTION 52
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 53
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 58
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 62
What component of the change management system is responsible for evaluating, testing, and documenting changes created to the project scope?

A. Scope Verification
B. Project Management Information System
C. Integrated Change Control
D. Configuration Management System

Answer: D

NEW QUESTION 66
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 70
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. A teaming agreement is an example of what risk response?

A. Mitigation
B. Sharing
C. Acceptance
D. Transference

Answer: B

NEW QUESTION 73
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 75
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 79
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 80
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 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 87
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 92
In which of the following SDLC phases is the system's security features configured and enabled, the system is tested and installed or fielded, and the system is authorized for processing?

A. Initiation Phase
B. Development/Acquisition Phase
C. Implementation Phase
D. Operation/Maintenance Phase

Answer: C

NEW QUESTION 97
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 99
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 101
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 106
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: B

NEW QUESTION 107
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 113
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: C

NEW QUESTION 116
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 117
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 119

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 120
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 125
Which of the following enables an inventor to legally enforce his right to exclude others from using his invention?

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

Answer: B

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: CD

NEW QUESTION 130
Which of the following statements best describes the consequences of the disaster recovery plan test?

A. If no deficiencies were found during the test, then the test was probably flawed.
B. The plan should not be changed no matter what the results of the test would be.
C. The results of the test should be kept secret.
D. If no deficiencies were found during the test, then the plan is probably perfec

Answer: A

NEW QUESTION 133
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 136
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: ABC

NEW QUESTION 140
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 145
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 149
What are the steps related to the vulnerability management program? Each correct answer represents a complete solution. Choose all that apply.

A. Maintain and Monitor
B. Organization Vulnerability
C. Define Policy
D. Baseline the Environment

Answer: ACD

NEW QUESTION 151
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 152
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 155
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 159
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 160
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 165
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 166
Which of the following administrative policy controls is usually associated with government classifications of materials and the clearances of individuals to access those materials?

A. Separation of Duties
B. Due Care
C. Acceptable Use
D. Need to Know

Answer: D

NEW QUESTION 171
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 173
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 178
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 182
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 184
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 187
Which of the following BCP teams handles financial arrangement, public relations, and media inquiries in the time of disaster recovery?

A. Software team
B. Off-site storage team
C. Applications team
D. Emergency-management team

Answer: D

NEW QUESTION 191
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 192
Fill in the blank with an appropriate phrase. is used to provide security mechanisms for the storage, processing, and transfer of data.

A. Data classification

Answer: A

NEW QUESTION 197
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 199
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

NEW QUESTION 203
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 208
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 211
Which of the following are the types of access controls? Each correct answer represents a complete solution. Choose three.

A. Administrative
B. Automatic
C. Physical
D. Technical

Answer: ACD

NEW QUESTION 214
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 216
A Web-based credit card company had collected financial and personal details of Mark before issuing him a credit card. The company has now provided Mark's financial and personal details to another company. Which of the following Internet laws has the credit card issuing company violated?

A. Copyright law
B. Trademark law
C. Privacy law
D. Security law

Answer: C

NEW QUESTION 217
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 219
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 220
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 225
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 227
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 230
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 231
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 resource

Answer: B

NEW QUESTION 235
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. Earned value management
B. Risk audit
C. Technical performance measurement
D. Correctiveaction

Answer: D

NEW QUESTION 236
How many change control systems are there in project management?

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

Answer: B

NEW QUESTION 239
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 241
Which of the following signatures watches for the connection attempts to well-known, frequently attacked ports?

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

Answer: A

NEW QUESTION 245
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

NEW QUESTION 246
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 247
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 248
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 250
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. Strict adherence to this Code is a condition of certification.
B. 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.
C. Advance and protect the profession.
D. Provide diligent and competent service to principal

Answer: AB

NEW QUESTION 253
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 258
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 261
Which of the following terms describes a repudiation of a contract that occurs before the time when performance is due?

A. Expected breach
B. Actual breach
C. Anticipatory breach
D. Nonperforming breach

Answer: C

NEW QUESTION 264
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 265
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 270
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 271
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 275
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 276
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 277
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. Electronic Communications Privacy Act of 1986
B. Wiretap Act
C. Computer Fraud and Abuse Act
D. Economic Espionage Act of 1996

Answer: A

NEW QUESTION 282
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 283
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 287
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: ABCD

NEW QUESTION 288
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 292
Which of the following is a variant with regard to Configuration Management?

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

Answer: C

NEW QUESTION 294
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 298
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 300
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 302
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: BD

NEW QUESTION 303
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 307
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 308
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 309
Which of the following processes is a structured approach to transitioning individuals, teams, and organizations from a current state to a desired future state?

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

Answer: C

NEW QUESTION 311
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 314
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 315
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. Vedit
C. Device Seizure
D. FAR system

Answer: D

NEW QUESTION 316
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 321
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 326
Which of the following methods can be helpful to eliminate social engineering threat? Each correct answer represents a complete solution. Choose three.

A. Password policies
B. Vulnerability assessments
C. Data encryption
D. Data classification

Answer: ABD

NEW QUESTION 330
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: A

NEW QUESTION 334
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 335
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 340
Which of the following are examples of administrative controls that involve all levels of employees within an organization and determine which users have access to what resources and information? Each correct answer represents a complete solution. Choose three.

A. Employee registration and accounting
B. Disaster preparedness and recovery plans
C. Network authentication
D. Training and awareness
E. Encryption

Answer: ABD

NEW QUESTION 343
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 345
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 347
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

NEW QUESTION 349
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. Communications management plan
B. Change management plan
C. Issue log
D. Risk management plan

Answer: B

NEW QUESTION 352
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 356
Which of the following refers to the ability to ensure that the data is not modified or tampered with?

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

Answer: C

NEW QUESTION 358
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 363
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 368
Fill in the blank with an appropriate word. are used in information security to formalize security policies.

A. Model

Answer: A

NEW QUESTION 370
Which of the following are known as the three laws of OPSEC? Each correct answer represents a part of the solution. Choose three.

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

Answer: ABC

NEW QUESTION 371
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 373

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 378
Which of the following is a name, symbol, or slogan with which a product is identified?

A. Copyright
B. Trademark
C. Trade secret
D. Patent

Answer: B

NEW QUESTION 380
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 385
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 388
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 389
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 393
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: BD

NEW QUESTION 396
......