ISC2

Exam Questions CISSP-ISSMP

Information Systems Security Management Professional

About Exambible

Your Partner of IT Exam

Found in 1998

Exambible is a company specialized on providing high quality IT exam practice study materials, especially Cisco CCNA, CCDA, CCNP, CCIE, Checkpoint CCSE, CompTIA A+, Network+ certification practice exams and so on. We guarantee that the candidates will not only pass any IT exam at the first attempt but also get profound understanding about the certificates they have got. There are so many alike companies in this industry, however, Exambible has its unique advantages that other companies could not achieve.

Our Advances

* 99.9% Uptime

All examinations will be up to date.

* 24/7 Quality Support

We will provide service round the clock.

* 100% Pass Rate

Our guarantee that you will pass the exam.

* Unique Gurantee

If you do not pass the exam at the first time, we will not only arrange FULL REFUND for you, but also provide you another exam of your claim, ABSOLUTELY FREE!

NEW QUESTION 1
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 2
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 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
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 5
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 6
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 7
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 8
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 9
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 10
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 13
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 14
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 17
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 21
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 23
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 25
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 26
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 28
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 32
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 36
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 38
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 42
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 44
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 45
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 50
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 55
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 60
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 63
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 64
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 67
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 72
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 75
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 79
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 82
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 86
Which of the following ports is the default port for Layer 2 Tunneling Protocol (L2TP) ?

A. UDP port 161
B. TCP port 443
C. TCP port 110
D. UDP port 1701

Answer: D

NEW QUESTION 91
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 92
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 96
Which of the following statements about the availability concept of Information security management is true?

A. It determines actions and behaviors of a single individual within a system.
B. It ensures reliable and timely access to resources.
C. It ensures that unauthorized modifications are not made to data byauthorized personnel or processes.
D. It ensures that modifications are not made to data by unauthorized personnel or processe

Answer: B

NEW QUESTION 100
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 101
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 105
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 109
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 112
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 116
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 118
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 123
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 125
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 130
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 135
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 138
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 140
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 145
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 147
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 151
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 152
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 153
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 154
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 155
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 157
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 161
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 163
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 167
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 168
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 169
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 174
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 176
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 178
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 181
What course of action can be taken by a party if the current negotiations fail and an agreement cannot be reached?

A. ZOPA
B. PON
C. Bias
D. BATNA

Answer: D

NEW QUESTION 184
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 188
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 189
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 191
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 194
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 199
You company suspects an employee of sending unauthorized emails to competitors. These emails are alleged to contain confidential company dat a. Which of the following is the most important step for you to take in preserving the chain of custody?

A. Preserve the email server including all logs.
B. Seize the employee's PC.
C. Make copies of that employee's email.
D. Place spyware on the employee's PC to confirm these activitie

Answer: A

NEW QUESTION 204
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 205
Which of the following is the default port for Simple Network Management Protocol (SNMP)?

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

Answer: C

NEW QUESTION 208
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 211
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 212
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 216
John is a black hat hacker. FBI arrested him while performing some email scams. Under which of the following US laws will john be charged?

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

Answer: B

NEW QUESTION 219
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 221
Which of the following types of cyber stalking damage the reputation of their victim and turn other people against them by setting up their own Websites, blogs or user pages for this purpose?

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

Answer: B

NEW QUESTION 225
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 229
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 232

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 234
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 238
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 242
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 246
You work as a security manager for SoftTech Inc. You are conducting a security awareness campaign for your employees. Which of the following ideas will you consider the best when
conducting a security awareness campaign?

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

Answer: C

NEW QUESTION 247
Which of the following measurements of an enterprise's security state is the process whereby an organization establishes the parameters within which programs, investments, and acquisitions reach the desired results?

A. Information sharing
B. Ethics
C. Performance measurement
D. Risk management

Answer: C

NEW QUESTION 251
Which of the following processes provides a standard set of activities, general tasks, and a management structure to certify and accredit systems, which maintain the information assurance and the security posture of a system or site?

A. NSA-IAM
B. DITSCAP
C. ASSET
D. NIACAP

Answer: D

NEW QUESTION 253
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 258
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 262
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 265
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 267
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 270
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 273
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 278
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 283
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 285
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 287
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 290
Which of the following concepts represent the three fundamental principles of information security? Each correct answer represents a complete solution. Choose three.

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

Answer: ABC

NEW QUESTION 292
.....

Relate Links

100% Pass Your CISSP-ISSMP Exam with Exambible Prep Materials

https://www.exambible.com/CISSP-ISSMP-exam/

Contact us

We are proud of our high-quality customer service, which serves you around the clock 24/7.

Viste - https://www.exambible.com/