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 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 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 3
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 4
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 5
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 6
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 7
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 8
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 9
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 10
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 10
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 15
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 17
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 20
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 21
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 22
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 27
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 28
Which of the following is a process of monitoring data packets that travel across a network?

A. Password guessing
B. Packet sniffing
C. Shielding
D. Packet filtering

Answer: B

NEW QUESTION 29
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 33
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 35
Which of the following statements best explains how encryption works on the Internet?

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

Answer: A

NEW QUESTION 37
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 41
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 45
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 48
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 53
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 54
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 59
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 60
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 63
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 65
How many change control systems are there in project management?

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

Answer: B

NEW QUESTION 69
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 74
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 77
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 80
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 85
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 90
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 93
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 94
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 95
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 99
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 103
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 105
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 106
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 107
You are the Network Administrator for a software company. Due to the nature of your company's business, you have a significant number of highly computer savvy users. However, you have still decided to limit each user access to only those resources required for their job, rather than give wider access to the technical users (such as tech support and software engineering personnel).
What is this an example of?

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

Answer: B

NEW QUESTION 111
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 113
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 116
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 121
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 125

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 127
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 130
Which of the following can be done over telephone lines, e-mail, instant messaging, and any other method of communication considered private.

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

Answer: C

NEW QUESTION 133
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 137
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 139
.....

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/