ISC2

Exam Questions 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 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 2
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 3
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 4
You are responsible for network and information security at a metropolitan police station. The most important concern is that unauthorized parties are not able to access data. What is this called?

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

Answer: D

NEW QUESTION 5
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 6
Which of the following acts is a specialized privacy bill that affects any educational institution to accept any form of funding from the federal government?

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

Answer: C

NEW QUESTION 7
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 8
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 9
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 10
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 10
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 11
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 14
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 16
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 17
Mark works as a security manager for SofTech Inc. He is working in a partially equipped office space which contains some of the system hardware, software, telecommunications, and power sources. In which of the following types of office sites is he working?

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

Answer: B

NEW QUESTION 22
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 23
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 24
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 29
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 30
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 32
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 35
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 38
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 42
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 43
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 45
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 47
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 51
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 55
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 60
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 61
Which of the following recovery plans includes specific strategies and actions to deal with specific variances to assumptions resulting in a particular security problem, emergency, or state of affairs?

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

Answer: B

NEW QUESTION 62
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 65
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 70
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 71
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 75
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 79
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 83
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 87
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 91
Which of the following are the responsibilities of the owner with regard to data in an information classification program? Each correct answer represents a complete solution. Choose three.

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

Answer: ABC

NEW QUESTION 96
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 98
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 103
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 105
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 110
How can you calculate the Annualized Loss Expectancy (ALE) that may occur due to a threat?

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

Answer: D

NEW QUESTION 114
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 119
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 124
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 127
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 130
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 132
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 136
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 140
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 141
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 146
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 149
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 150
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 155
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 160
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 165
Management has asked you to perform a risk audit and report back on the results. Bonny, a project team member asks you what a risk audit is. What do you tell Bonny?

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

Answer: B

NEW QUESTION 170
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 171
Which of the following SDLC phases consists of the given security controls. Misuse Case Modeling Security Design and Architecture Review Threat and Risk Modeling Security Requirements and Test Cases Generation

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

Answer: A

NEW QUESTION 175
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 177
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 178
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 182
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 185
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 190
Fill in the blank with an appropriate word. are used in information security to formalize security policies.

A. Model

Answer: A

NEW QUESTION 191
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 192
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 195
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 199
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 200
.....

Relate Links

100% Pass Your ISSMP Exam with Exambible Prep Materials

https://www.exambible.com/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/