Actual4Dump

Choose the version that fits your needs	PDF Version	Desktop Test Engine	Online Test Engine
Latest and Up-to-Date exam dumps with real exam questions answers.	✓	✓	✓
Get 12-Months free updates without any extra charges.	✓	✓	✓
Experience same exam environment before appearing in the certification exam.	✗	✓	✓
100% exam passing guarante in the first attempt.	✓	✓	✓
20% discount on more than one license and 30% discount on 5+ license purchases.	✗	✓	✓
100% secure purchase on SSL.	✓	✓	✓
Completely private purchase without sharing your personal info with anyone.	✓	✓	✓

http://www.actual4dump.com

Superb Exam Dumps Materials lead you to get your certification easily - Actual4dump

Exam : CSSLP

Title : Certified Secure Software Lifecycle Professional Practice Test

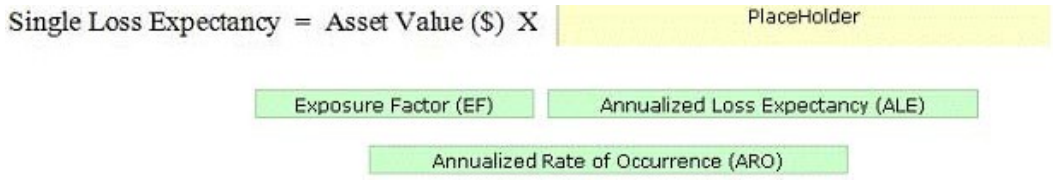
Vendors : ISC

Version : DEMO

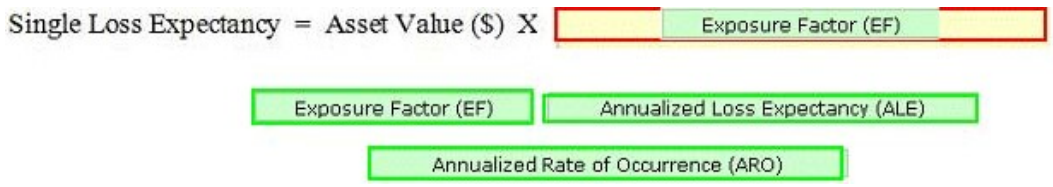
1.You work as a Network Auditor for Net Perfect Inc. The company has a Windows-based network. While auditing the company's network, you are facing problems in searching the faults and other entities that belong to it. Which of the following risks may occur due to the existence of these problems?
A. Residual risk
B. Secondary risk
C. Detection risk
D. Inherent risk
Answer: C

2.The National Information Assurance Certification and Accreditation Process (NIACAP) is the minimum standard process for the certification and accreditation of computer and telecommunications systems that handle U.S. national security information. Which of the following participants are required in a NIACAP security assessment.?
Each correct answer represents a part of the solution. Choose all that apply.
A. Certification agent
B. Designated Approving Authority
C. IS program manager
D. Information Assurance Manager
E. User representative
Answer: A,B,C,E

3.DRAG DROP
Drop the appropriate value to complete the formula.



Answer:



4.Which of the following penetration testing techniques automatically tests every phone line in an exchange and tries to locate modems that are attached to the network?
A. Demon dialing
B. Sniffing
C. Social engineering
D. Dumpster diving
Answer: A

5.Which of the following roles is also known as the accreditor?

A. Data owner
B. Chief Risk Officer
C. Chief Information Officer
D. Designated Approving Authority
Answer: D

6.DoD 8500.2 establishes IA controls for information systems according to the Mission Assurance Categories (MAC) and confidentiality levels. Which of the following MAC levels requires high integrity and medium availability?
A. MAC III
B. MAC IV
C. MAC I
D. MAC II
Answer: D

7.Microsoft software security expert Michael Howard defines some heuristics for determining code review in "A Process for Performing Security Code Reviews". Which of the following heuristics increase the application's attack surface? Each correct answer represents a complete solution. Choose all that apply.
A. Code written in C/C++/assembly language
B. Code listening on a globally accessible network interface
C. Code that changes frequently
D. Anonymously accessible code
E. Code that runs by default
F. Code that runs in elevated context
Answer: B,D,E,F

8 .Which of the following cryptographic system services ensures that information will not be disclosed to any unauthorized person on a local network?
A. Authentication
B. Integrity
C. Non-repudiation
D. Confidentiality
Answer: D

9.What are the various activities performed in the planning phase of the Software Assurance Acquisition process? Each correct answer represents a complete solution. Choose all that apply.
A. Develop software requirements.
B. Implement change control procedures.
C. Develop evaluation criteria and evaluation plan.
D. Create acquisition strategy.
Answer: A,C,D

10.You work as a project manager for BlueWell Inc. You are working on a project and the management wants a rapid and cost-effective means for establishing priorities for planning risk responses in your

project. Which risk management process can satisfy management's objective for your project?
A. Qualitative risk analysis
B. Historical information
C. Rolling wave planning
D. Quantitative analysis
Answer: A

11.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. Biba Integrity Model
C. Bell-LaPadula Model
D. Access Matrix
Answer: A

12.You are the project manager for GHY Project and are working to create a risk response for a negative risk. You and the project team have identified the risk that the project may not complete on time, as required by the management, due to the creation of the user guide for the software you're creating. You have elected to hire an external writer in order to satisfy the requirements and to alleviate the risk event. What type of risk response have you elected to use in this instance?
A. Transference
B. Exploiting
C. Avoidance
D. Sharing
Answer: A

13.Which of the following organizations assists the President in overseeing the preparation of the federal budget and to supervise its administration in Executive Branch agencies?
A. OMB
B. NIST
C. NSA/CSS
D. DCAA
Answer: A

14.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 Identification
B. Configuration Verification and Auditing
C. Configuration Status Accounting
D. Configuration Item Costing
Answer: D

15.Which of the following types of redundancy prevents attacks in which an attacker can get physical control of a machine, insert unauthorized software, and alter data?
A. Data redundancy
B. Hardware redundancy
C. Process redundancy
D. Application redundancy
Answer: C

16.Which of the following individuals inspects whether the security policies, standards, guidelines, and procedures are efficiently performed in accordance with the company's stated security objectives?
A. Information system security professional
B. Data owner
C. Senior management
D. Information system auditor
Answer: D

17.Which of the following process areas does the SSE-CMM define in the 'Project and Organizational Practices' category? Each correct answer represents a complete solution. Choose all that apply.
A. Provide Ongoing Skills and Knowledge
B. Verify and Validate Security
C. Manage Project Risk
D. Improve Organization's System Engineering Process
Answer: A,C,D

18.The LeGrand Vulnerability-Oriented Risk Management method is based on vulnerability analysis and consists of four principle steps. Which of the following processes does the risk assessment step include? Each correct answer represents a part of the solution. Choose all that apply.
A. Remediation of a particular vulnerability
B. Cost-benefit examination of countermeasures
C. Identification of vulnerabilities
D. Assessment of attacks
Answer: B,C,D

19.You work as a Security Manager for Tech Perfect Inc. You have set up a SIEM server for the following purposes: Analyze the data from different log sources Correlate the events among the log entries Identify and prioritize significant events Initiate responses to events if required One of your log monitoring staff wants to know the features of SIEM product that will help them in these purposes. What features will you recommend? Each correct answer represents a complete solution. Choose all that apply.
A. Asset information storage and correlation
B. Transmission confidentiality protection
C. Incident tracking and reporting
D. Security knowledge base
E. Graphical user interface
Answer: A,C,D,E

20.According to U.S. Department of Defense (DoD) Instruction 8500.2, there are eight Information Assurance (IA) areas, and the controls are referred to as IA controls. Which of the following are among the eight areas of IA defined by DoD? Each correct answer represents a complete solution. Choose all that apply.
A. VI Vulnerability and Incident Management
B. Information systems acquisition, development, and maintenance
C. DC Security Design & Configuration
D. EC Enclave and Computing Environment
Answer: A,C,D

21.The Information System Security Officer (ISSO) and Information System Security Engineer (ISSE) play the role of a supporter and advisor, respectively. Which of the following statements are true about ISSO and ISSE? Each correct answer represents a complete solution. Choose all that apply.
A. An ISSE manages the security of the information system that is slated for Certification & Accreditation (C&A).
B. An ISSE provides advice on the continuous monitoring of the information system.
C. An ISSO manages the security of the information system that is slated for Certification & Accreditation (C&A).
D. An ISSE provides advice on the impacts of system changes. E. An ISSO takes part in the development activities that are required to implement system changes.
Answer: B,C,D

22.In which of the following types of tests are the disaster recovery checklists distributed to the members of disaster recovery team and asked to review the assigned checklist?
A. Parallel test
B. Simulation test
C. Full-interruption test
D. Checklist test
Answer: D

23.CORRECT TEXT
Fill in the blank with an appropriate phrase. models address specifications, requirements, design, verification and validation, and maintenance activities.
A. Life cycle
Answer: A

24.Which of the following security design patterns provides an alternative by requiring that a user's authentication credentials be verified by the database before providing access to that user's data?
A. Secure assertion
B. Authenticated session
C. Password propagation
D. Account lockout
Answer: C

25.Which of the following is the duration of time and a service level within which a business process must be restored after a disaster in order to avoid unacceptable consequences associated with a break in business continuity?
A. RTO
B. RTA
C. RPO
D. RCO
Answer: A

26.Which of the following processes culminates in an agreement between key players that a system in its current configuration and operation provides adequate protection controls?
A. Information Assurance (IA)
B. Information systems security engineering (ISSE)
C. Certification and accreditation (C&A)
D. Risk Management
Answer: C

27.Adam works as a Computer Hacking Forensic Investigator for a garment company in the United States. A project has been assigned to him to investigate a case of a disloyal employee who is suspected of stealing design of the garments, which belongs to the company and selling those garments of the same design under different brand name. Adam investigated that the company does not have any policy related to the copy of design of the garments. He also investigated that the trademark under which the employee is selling the garments is almost identical to the original trademark of the company. On the grounds of which of the following laws can the employee be prosecuted?
A. Espionage law
B. Trademark law
C. Cyber law
D. Copyright law
Answer: B

28.John works as a professional Ethical Hacker. He has been assigned the project of testing the security of www.we-are-secure.com. In order to do so, he performs the following steps of the pre-attack phase successfully: Information gathering Determination of network range Identification of active systems Location of open ports and applications Now, which of the following tasks should he perform next?
A. Perform OS fingerprinting on the We-are-secure network.
B. Map the network of We-are-secure Inc.
C. Install a backdoor to log in remotely on the We-are-secure server.
D. Fingerprint the services running on the we-are-secure network.
Answer: A

29.Which of the following DITSCAP C&A phases takes place between the signing of the initial version of the SSAA and the formal accreditation of the system?
A. Phase 4

B. Phase 3
C. Phase 1
D. Phase 2
Answer: D

30.In which of the following testing methodologies do assessors use all available documentation and work under no constraints, and attempt to circumvent the security features of an information system?
A. Full operational test
B. Penetration test
C. Paper test
D. Walk-through test
Answer: B