KillTest

Higher Quality, Better Service!

Q&A

http://www.killtest.com

We offer free update service for one year.

Exam : **G2700**

Title : GIAC Certified ISO-2700 Specialist Practice Test

Version : Demo

1.Mark works as a Network Security Administrator for uCertify Inc. An employee of the organization comes to Mark and tells him that a few months ago, the employee had filled an online bank form due to some account related work. Today, when again visiting the site, the employee finds that some of his personal information is still being displayed in the webpage. Which of the following types of cookies should be disabled by Mark to resolve the issue?
A. Session
B. Temporary
C. Secure
D. Persistent
Answer: D

2.You work as an Information Security Manager for uCertify Inc. You are working on the documentation of control A.10.1.1. What is the purpose of control A.10.1.1.?
A. It is concerned with the documentation of the human resource security to make recruitments clear to the organization.
B. It is concerned with the documentation of the supply chain management.
C. It is concerned with the documentation of operating procedures to ensure the correct and secure use of information processing facilities.
D. It is concerned with the documentation of the disaster recovery management to ensure proper backup technologies.
Answer: C

3.Mark works as a Network Security Administrator for uCertify Inc. He has been assigned the task of installing a MySQL server. Mark wants to monitor only the data that is directed to or originating from the server and he also wants to monitor running processes, file system access and integrity, and user logins for identifying malicious activities. Which of the following intrusion detection techniques will Mark use to accomplish the task?
A. Network-based IDS
B. Signature-based IDS
C. Anomaly-based IDS
D. Host-based IDS
Answer: D

4.Which of the following are the exceptions of the Data Protection Act?
Each correct answer represents a complete solution. Choose all that apply.
A. Section 36 - Domestic purposes
B. Section 28 - National security
C. Section 55 - Unlawful obtaining of personal data
D. Section 29 - Crime and taxation
Answer: A,B,D

5.Which of the following statements are true about security risks?
Each correct answer represents a complete solution. Choose three.
A. These are considered as an indicator of threats coupled with vulnerability.

B. These can be removed completely by taking proper actions.
C. These can be mitigated by reviewing and taking responsible actions based on possible risks.
D. These can be analyzed and measured by the risk analysis process.
Answer: A,C,D

6.A project plan includes the Work Breakdown Structure (WBS) and cost estimates. Which of the following are the parts of a project plan?
Each correct answer represents a complete solution. Choose all that apply.
A. Risk identification
B. Security Threat
C. Project schedule
D. Team members list
E. Risk analysis
Answer: A,C,D,E

7.Which of the following are the basics of Business Continuity Management?
Each correct answer represents a complete solution. Choose all that apply.
A. Implementation of a risk assessment technique to identify the causes and consequences of failures
B. Regular checking of business continuity plans
C. Identification of authentication techniques according to the requirements
D. Identification of human resources according to the requirements
Answer: A,B,D

8.Which of the following controls are administrative in nature?
A. Directive controls
B. Recovery controls
C. Preventive controls
D. Detective controls
Answer: A

9.CORRECT TEXT
Fill in the blank with an appropriate phrase.
_____accord describes the minimum regulatory capital to be allocated by each bank based on its risk profile of assets.
Answer: Basel ll

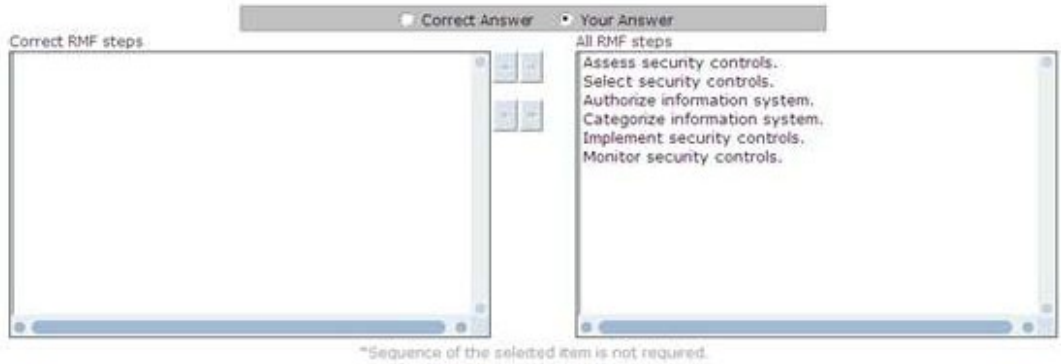
10.You work as an Information Security Officer for uCertify Inc. You need to create an asset management plan differentiating fixed assets from inventory items. How will you differentiate assets from inventory items?
A. Inventory items are sold.
B. Assets are temporary usually.
C. Inventory items are permanent.
D. Assets cannot be used.
Answer: A

11.Which of the following is a Restrict Anonymous registry value that allows users with explicit anonymous permissions?
A. 2
B. 3
C. 1
D. 0
Answer: A

12.Rick works as a Computer Forensic Investigator for BlueWells Inc. He has been informed that some confidential information is being leaked out by an employee of the company. Rick suspects that someone is sending the information through email. He checks the emails sent by some employees to other networks. Rick finds out that Sam, an employee of the Sales department, is continuously sending text files that contain special symbols, graphics, and signs. Rick suspects that Sam is using the Steganography technique to send data in a disguised form. Which of the following techniques is Sam using?
Each correct answer represents a part of the solution. Choose all that apply.
A. Linguistic steganography
B. Text Semagrams
C. Technical steganography
D. Perceptual masking
Answer: A,B

13.CORRECT TEXT
Fill in the blank with the appropriate term.
_____ is a powerful and low-interaction open source honeypot.
Answer: Honeyd

14.The disciplined and structured process, that integrates information security and risk management activities into the System Development Life Cycle, is provided by the risk management framework. Choose the appropriate RMF steps.
A.



Answer: A

15.Mark works as an Office Assistant for uCertify Inc. He is responsible for managing office documents. Today, after opening a word document, Mark noticed that the other opened documents are closed

suddenly. After reopening those documents, Mark found some modifications in the documents. He contacted his Security Administrator and came to know that there is a virus program installed in the operating system. Which of the following types of virus has attacked the operating system?
A. Data file
B. Macro
C. Polymorphic
D. Boot sector
Answer: A

16.Which of the following should be considered while calculating the costs of the outage?
Each correct answer represents a complete solution. Choose all that apply.
A. Sales aspect of the business
B. Cost of low productivity
C. Innovations in electronic funds transfer
D. Cost of lost income from missed sales
Answer: B,D

17.Which of the following phases of the PDCA model is the monitoring and controlling phase of the Information Security Management System (ISMS)?
A. Check
B. Plan
C. Do
D. Act
Answer: A

18.Mark works as a System Administrator for uCertify Inc. He is responsible for securing the network of the organization. He is configuring some of the advanced features of the Windows firewall so that he can block the client machine from responding to pings. Which of the following advanced setting types should Mark change for accomplishing the task?
A. ICMP
B. SNMP
C. UDP
D. SMTP
Answer: A

19.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

20.Which of the following is a fast-emerging global sector that advises individuals and corporations on

how to apply the highest ethical standards to every aspect of their business?
A. Service Capacity Management (SCM)
B. Business Capacity Management (BCM)
C. Resource Capacity Management (RCM)
D. Integrity Management Consulting
Answer: D

21.You work as an Information Security Manager for uCertify Inc. You are working on communication and organization management. You need to create the documentation on change management.
Which of the following are the main objectives of change management?
Each correct answer represents a complete solution. Choose all that apply.
A. Minimal disruption of services
B. Reduction of inventory in accordance with revenue
C. Economic utilization of resources involved in the change
D. Reduction in back-out activities
Answer: A,C,D

22.Which of the following is used for secure financial transactions over the Internet?
A. ATM
B. VPN
C. SSL
D. SET
Answer: D

23.You work as a Security Administrator for uCertify Inc. You have been assigned the task to verify the identity of the employees recruited in your organization. Which of the following components of security deals with an employee's verification in the organization?
A. Network Security
B. Physical security
C. Access security
D. Human resource security
Answer: D

24.You work as the Human Resource Manager for uCertify Inc. You need to recruit some candidates for the marketing department of the organization. Which of the following should be defined to the new employees of the organization before they have joined?
Each correct answer represents a complete solution. Choose all that apply.
A. Marketing tips and tricks
B. Organization's network topology
C. Job roles
D. Organization's security policy
Answer: C,D

25.You work as an Information Security Manager for uCertify Inc. You need to make the

documentation on change management. What are the advantages of change management?
Each correct answer represents a complete solution. Choose all that apply.
A. Improved productivity of users due to more stable and better IT services
B. Improved IT personnel productivity, since there is a reduced number of urgent changes and a back-out of erroneous changes
C. Improved adverse impact of changes on the quality of IT services
D. Increased ability to absorb frequent changes without making an unstable IT environment
Answer: A,B,D

26.You work as a Network Administrator for uCertify Inc. The organization has constructed a cafeteria for their employees and you are responsible to select the access control method for the cafeteria.
There are a few conditions for giving access to the employees, which are as follows:
1. Top level management can get access any time.
2. Staff members can get access during the specified hours.
3. Guests can get access only in working hours.
Which of the following access control methods is suitable to accomplish the task?
A. Discretionary access control
B. Lattice-based access control
C. Attribute-based access control
D. Rule-based access control
Answer: D

27.Which of the following are the uses of cryptography as defined in a policy document?
Each correct answer represents a complete solution. Choose all that apply.
A. Backup
B. Control of keys
C. Applications supporting cryptography
D. Recovery
Answer: A,B,C

28.Which of the following is the designing phase of the ISMS?
A. Check
B. Plan
C. Act
D. Do
Answer: B

29.Single Loss Expectancy (SLE) represents an organization's loss from a single threat. Which of the following formulas best describes the Single Loss Expectancy (SLE)?
A. SLE = Asset Value (AV) * Exposure Factor (EF)
B. SLE = Annualized Loss Expectancy (ALE) * Exposure Factor (EF)
C. SLE = Annualized Loss Expectancy (ALE) * Annualized Rate of Occurrence (ARO)
D. SLE = Asset Value (AV) * Annualized Rate of Occurrence (ARO)
Answer: A

30.Qualitative risk analysis includes judgment, intuition, and experience. Which of the following methods are used to perform qualitative risk analysis?
Each correct answer represents a complete solution. Choose all that apply.
A. Egress filtering
B. Checklists
C. Delphi technique
D. Brainstorming
Answer: B,C,D