GIAC

Exam G2700

GIAC Certified ISO-2700 Specialist Practice Test

Version: 6.0

[Total Questions: 453]

Topic break down

Topic	No. of Questions
Topic 1: Volume A	100
Topic 2: Volume B	100
Topic 3: Volume C	100
Topic 4: Volume D	153

Topic 1, Volume A

Question No : 1 - (Topic 1)

You work as an Information Security Manager for uCertify Inc. You are working on a document regarding the PDCA methodology. Which of the following elements of the PDCA (Plan-Do-Check- Act) methodology is used to continually improve the process performance?

A. Act
B. Check
C. Do
D. Plan

Answer: A

Question No : 2 - (Topic 1)

You work as an Information Security Manager for uCertify Inc. The company has made a contract with a third party software company to make a software program for personal use. You have been assigned the task to share the organization's personal requirements regarding the tool to the third party. Which of the following documents should be first signed by the third party?

A. Non disclosure agreement (NDA)
B. Acknowledgement papers
C. Copyright papers
D. Legal disclaimer

Answer: A

Question No : 3 - (Topic 1)

Which of the following are the variables on which the structure of Service Level Agreement depends?

Each correct answer represents a complete solution. Choose all that apply.

A. It depends on the cultural aspects.
B. It depends on the infrastructure aspects of the organization.
C. It depends on the nature of the business activities, in terms of general terms and conditions, and business hours.
D. It depends on the physical aspects of the organization.

Answer: A,C,D

Question No : 4 - (Topic 1)

Which of the following is an authentication scheme used by Point to Point Protocol (PPP) servers to validate the identity of remote clients?

A. BGP
B. SMTP
C. CHAP
D. DHCP

Answer: C

Question No : 5 - (Topic 1)

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

Question No : 6 - (Topic 1)

Which of the following types of attack can be used to break the best physical and logical

security mechanism to gain access to a system?

A. Mail bombing
B. Cross site scripting attack
C. Social engineering attack
D. Password guessing attack

Answer: C

Question No : 7 - (Topic 1)

You work as an Information Security Manager for uCertify Inc. You have been assigned the task to create the documentation on control A.7.2 of the ISO standard. Which of the following is the chief concern of control A.7.2?

A. Classification of owners
B. Usage of information
C. Identification of inventory
D. Classification of information

Answer: D

Question No : 8 - (Topic 1)

You work as a Security Administrator for uCertify Inc. You have been assigned a task to implement information classification levels. You want to put the highly sensitive documents that should only be accessed by few people of the organization. In which of the following information classification levels should you put those documents?

A. Department specific
B. High security levels
C. Not to be copied
D. Classified

Answer: B

Question No : 9 - (Topic 1)

Which of the following are the perspectives considered to ensure the confidentiality, integrity, and availability of an organization's assets, information, data, and IT services?

Each correct answer represents a complete solution. Choose all that apply.

A. Procedural
B. Technical
C. Management
D. Organizational

Answer: A,B,D

Question No : 10 CORRECT TEXT - (Topic 1)

Fill in the blank with the appropriate term.

_____is the built-in file encryption tool for Windows file systems. It protects encrypted files from those who have physical possession of the computer where the encrypted files are stored.

Answer: EFS

Question No : 11 - (Topic 1)

Which of the following operations are performed by the Identity Management Process?

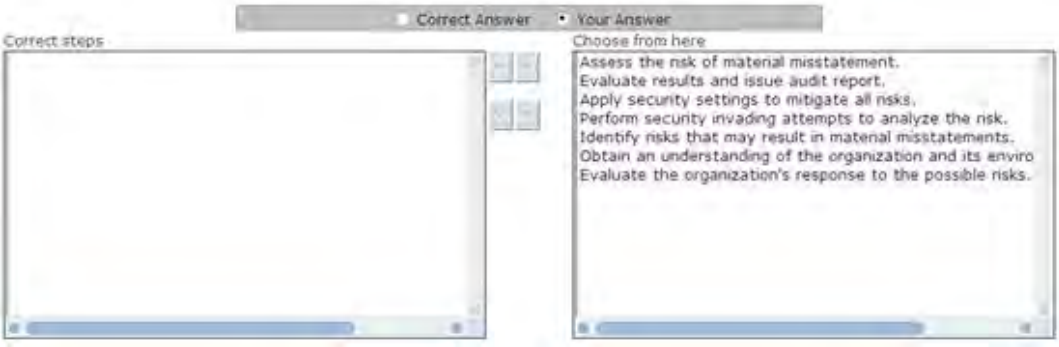
Each correct answer represents a complete solution. Choose all that apply.

A. Providing Single Sign-On access
B. Making possible automated application provision
C. Provisioning and coordinating user identities
D. Ensuring secure deployment of applications

Answer: A,B,C,D

Question No : 12 - (Topic 1)

Choose and reorder the appropriate steps that you will take to perform auditing.



A.

Answer: A

Question No : 13 CORRECT TEXT - (Topic 1)

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 II

Question No : 14 - (Topic 1)

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

Question No : 15 - (Topic 1)

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

Question No : 16 - (Topic 1)

Which of the following is the element used in the technology of encrypting and decrypting the text in cryptography?

A. Cipher
B. Key
C. Plaintext
D. Encryption

Answer: B

Question No : 17 - (Topic 1)

The Information Security Officer (ISO) of Blue Well Inc. wants to have a list of security measures put together. What should be done before security measures are selected by the Information Security Officer?

A. Carry out a risk analysis.
B. Formulate information security policy.
C. Set up monitoring.
D. Carry out an evaluation.

Answer: A

Question No : 18 - (Topic 1)

Which of the following plans provides measures and capabilities for recovering a major application or general support system?

A. Disaster recovery plan
B. Crisis communication plan
C. Contingency plan
D. Business continuity plan

Answer: C

Question No : 19 - (Topic 1)

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

Question No : 20 - (Topic 1)

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

Question No : 21 - (Topic 1)

Which of the following standards was made in 1995 by the joint initiative of the Department of Trade and Industry in the United Kingdom and leading UK private-sector businesses?

A. BS7799
B. ISO 27001
C. BS2700
D. ISMS

Answer: A

Question No : 22 - (Topic 1)

David works as the Chief Information Security Officer for uCertify Inc. Which of the following are the responsibilities that should be handled by David?

Each correct answer represents a complete solution. Choose all that apply.

A. Information security
B. Information risk management
C. Information privacy
D. Information development

Answer: A,B,C

Question No : 23 - (Topic 1)

Which of the following are features of protocol and spectrum analyzers?

Each correct answer represents a complete solution. Choose all that apply.

A. A protocol analyzer can identify physical layer errors in a network switch.
B. A packet analyzer can be used to capture real-time packets and can monitor the network packets on the LAN and the Internet.
C. A protocol analyzer can be used to analyze network traffic to trace specific transactions.
D. A spectrum analyzer should have the sensitive measuring equipment capability for detecting waveform frequencies and can identify and locate the interfering transmitter.

Answer: B,C,D

Question No : 24 - (Topic 1)

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

Question No : 25 - (Topic 1)

Which of the following are the factors that determine the degree to which the Return on Investment overstates the economic value?

Each correct answer represents a complete solution. Choose all that apply.

A. Capitalization policy
B. Growth rate of new investment
C. Growth rate of old investment
D. Length of project life

Answer: A,B,D

Question No : 26 - (Topic 1)

Which of the following information security standards deals with the protection of the computer facilities?

A. Physical and environmental security
B. Compliance
C. Organization of information security
D. Risk assessment and treatment

Answer: A

Question No : 27 - (Topic 1)

Which of the following are the things included by sensitive system isolation?

Each correct answer represents a complete solution. Choose all that apply.

A. Construction of appropriately isolated environments where technically and operationally feasible
B. Inclusion of all documents technically stored in a virtual directory
C. Explicit identification and acceptance of risks when shared facilities and/or resources must be used
D. Explicit identification and documentation of sensitivity by each system/application controller (owner)

Answer: A,C,D

Question No : 28 - (Topic 1)

Andrew is the CEO of uCertify Inc. He wants to improve the resources and revenue of the company. He uses the PDCA methodology to accomplish the task. Which of the following are the phases of the PDCA methodology?

Each correct answer represents a complete solution. Choose all that apply.

A. Deviate
B. Plan
C. Calculate
D. Act

Answer: B,D

Question No : 29 - (Topic 1)

Which of the following statements about incremental backup are true?

Each correct answer represents a complete solution. Choose two.

A. It backs up only the files changed since the most recent backup and clears the archive bit.
B. It is the fastest method of backing up data.
C. It is the slowest method for taking a data backup.
D. It backs up the entire database, including the transaction log.

Answer: A,B

Question No : 30 - (Topic 1)

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

Question No : 31 - (Topic 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

Question No : 32 - (Topic 1)

Which of the following is the designing phase of the ISMS?

A. Check
B. Plan
C. Act
D. Do

Answer: B

Question No : 33 - (Topic 1)

Which of the following tasks are performed by Information Security Management?

Each correct answer represents a complete solution. Choose all that apply.

A. It is designed to protect information and any equipment that is used in connection with its storage, transmission, and processing.
B. It is designed to develop information and any equipment that is used in connection with its storage, transmission, and processing.
C. It is designed to recognize information and any equipment that is used in connection with its storage, transmission, and processing.
D. It is designed to control information and any equipment that is used in connection with its storage, transmission, and processing.

Answer: A,C,D

Question No : 34 - (Topic 1)

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

Question No : 35 - (Topic 1)

Victor wants to send an encrypted message to his friend. He is using a steganography technique to accomplish his task. He takes a cover object and changes it accordingly to hide information.

This secret information is recovered only when the algorithm compares the changed cover with the original cover. Which of the following steganography methods is Victor using to accomplish his task?

A. The distortion technique
B. The substitution technique
C. The cover generation technique
D. The spread spectrum technique

Answer: A

Question No : 36 - (Topic 1)

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.