Vendor: GIAC

Exam Code: G2700

Exam Name: GIAC Certified ISO-2700 Specialist Practice Test

Version: Demo

QUESTION NO: 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: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 8

Which of the following controls are administrative in nature?

A. Directive controls
B. Recovery controls
C. Preventive controls
D. Detective controls

Answer: A

QUESTION NO: 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 II

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 13 CORRECT TEXT

Fill in the blank with the appropriate term.

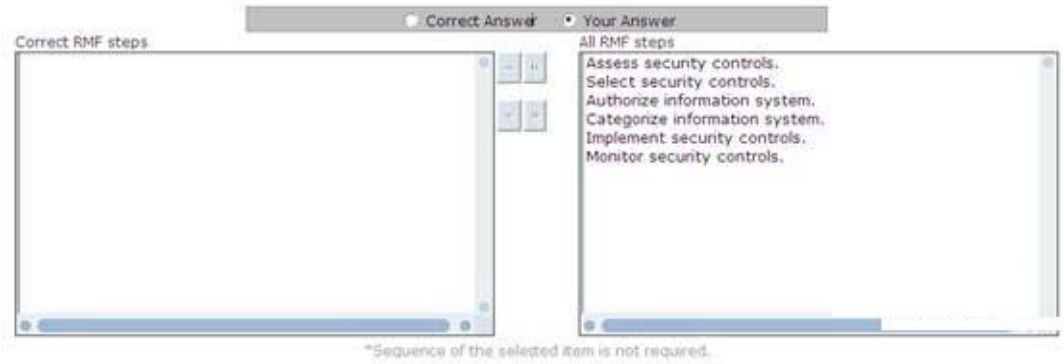
_____ is a powerful and low-interaction open source honeypot.

Answer: Honeyd

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 22

Which of the following is used for *secure financial transactions* over the Internet?

A. ATM
B. VPN
C. SSL
D. SET

Answer: D

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 28

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

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

Answer: B

QUESTION NO: 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

QUESTION NO: 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

QUESTION NO: 31

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: 32

Which of the following is a technical measure?

A. Encryption of data
B. Creation of a policy that defines what is and what is not permitted in the e-mail
C. Allocation of information to an owner
D. Storage of system management passwords

Answer: A

QUESTION NO: 33

Which of the following types of social engineering attacks is a term that refers to going through someone's trash to find out useful or confidential information?

A. Authorization by third party

B. Dumpster diving
C. Shoulder surfing
D. Important user posing

Answer: B

QUESTION NO: 34

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: 35

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You need to assign ownership of some assets of the organization. Which of the following statements correctly describe the responsibilities of an asset owner?

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

A. The owner has property rights to the asset.
B. The owner is allowed to delegate responsibility for maintaining the asset.
C. The owner should have a document describing the security controls for the asset.
D. The owner is allowed to delegate accountability of the asset.

Answer: B,C

QUESTION NO: 36

You work as a Security Administrator for uCertify Inc. You need to make a documentation to provide ongoing education and awareness training of disciplinary actions of your company. What are the primary reasons to create this documentation?

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

A. To ensure that employees understand information security threats
B. To ensure that employees have the necessary knowledge to mitigate security threats
C. To ensure that employees are aware of and understand their roles and responsibilities
D. To ensure that employees have the necessary knowledge about the company's forthcoming Projects

Answer: A,B,C

QUESTION NO: 37

The stronger points of CRAMM assist prioritization by providing a countermeasure with high priority if some conditions are met. Which of the following are these conditions?

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

A. It requires protecting a high risk system.
B. It does not require the installation of alternative countermeasures.
C. It is inexpensive to implement.
D. It provides protection against several threats.

Answer: A,B,D

QUESTION NO: 38

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: 39

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: 40

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: 41

Which of the following is one of the mechanisms available for administrators to employ for replicating the databases containing the DNS data across a set of DNS servers?

A. DNS zone transfer
B. DNS cache poisoning
C. DNS spoofing
D. ARP spoofing

Answer: A

QUESTION NO: 42

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You need to differentiate various assets of your organization. Which of the following are information assets?

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

A. User manuals
B. Operating systems
C. Training metarials
D. Personal data

Answer: A,C,D

QUESTION NO: 43 CORRECT TEXT

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: 44

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 identification
D. Risk control

Answer: C,D

QUESTION NO: 45

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: 46

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: 47

Which of the following international information security standards is concerned with anticipating and responding to information security breaches?

A. Organization of information security
B. Information security incident management
C. Physical and environmental security
D. Risk assessment and treatment

Answer: B

QUESTION NO: 48

You work as the Network Security Administrator for uCertify Inc. You are responsible for protecting your network from unauthorized access from both inside and outside the organization. For outside attacks, you have installed a number of security tools that protect your network. For internal security, employees are using passwords more than 8 characters; however, a few of them having the same designation often exchange their passwords, making it possible for others to access their accounts.

There is already a policy to stop this practice, but still employees are doing so. Now, you want to stop this and ensure that this never happens again. Which of the following will be the best step to stop this practice?

A. Create a policy that forces users to create a password combined with special characters.
B. Create a new policy that forces users to change their passwords once every 15 days.
C. Create a policy to enter their employee code while logged in to the system.
D. Create a policy to enter their personal email id while logged in to the system.

Answer: B

QUESTION NO: 49

You work as a Project Manager for uCertify Inc. You are working on an asset management plan.

You need to make the documentation on every single process related to asset management.

Which of the following is an example of asset management?

A. Making DR plan
B. Tracking references
C. Checking topology
D. Tracking inventory

Answer: D

QUESTION NO: 50

In which of the following does CRAMM provide assistance?

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

A. Audits
B. Contingency planning
C. US7799 certification
D. BS7799 certification

Answer: A,B,D

QUESTION NO: 51

You work as an Information Security Manager for uCertify Inc. You are working on a project related to communications and operations management. Which of the following controls of the ISO standard is concerned with operational procedures and responsibilities?

A. Control A.10.1
B. Control A.7.1
C. Control A.8.1
D. Control A.9.2

Answer: A

QUESTION NO: 52

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: 53

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: 54

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 owner
B. Data custodian
C. Auditor
D. User

Answer: C

QUESTION NO: 55

Mark works as a Security Administrator for uCertify Inc. For the last few days, he is getting an error message, i.e., 'Remove the Boot.ini file because it is harmful for operating system'. When Mark reads about the Boot.ini file, he finds that it is a system file that is used to load the operating system on a computer. Which of the following types of virus has attacked Mark's computer?

A. Polymorphic
B. Hoax
C. Macro
D. Multipartite

Answer: B

QUESTION NO: 56

Which of the following Acts enacted in the United States allows the FBI to issue National Security Letters (NSLs) to Internet service providers (ISPs) ordering them to disclose records about their customers?

A. Wiretap Act
B. Electronic Communications Privacy Act of 1986
C. Economic Espionage Act of 1996
D. Computer Fraud and Abuse Act

Answer: B

QUESTION NO: 57

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

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

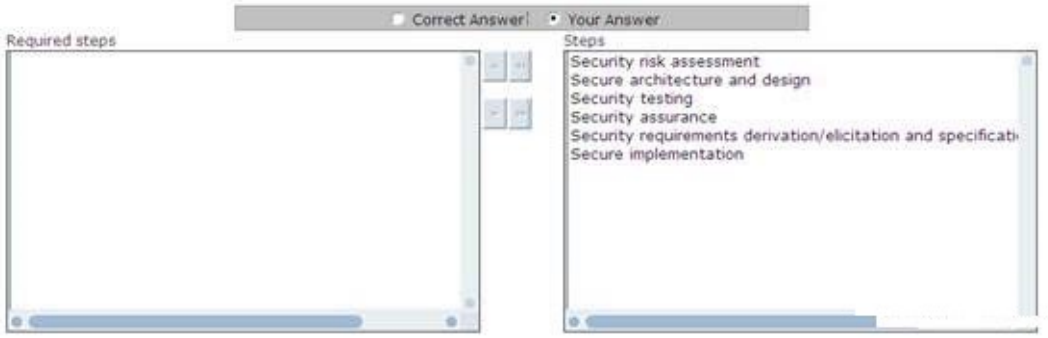
A. Providing Single Sign-On access
B. Making possible automated application provision

C. Provisioning and coordinating user identities
D. Ensuring secure deployment of applications

Answer: A,B,C,D

QUESTION NO: 58

Cigital Risk Management Method was developed by Gary McGraw of Cigital and John Viega of Stonewall Software, and it defines software security risk management process. Choose and re-order the risk management steps that are included in this method.



A.

Answer: A

QUESTION NO: 59

Which of the following are the two methods that are commonly used for applying mandatory access control?

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

A. Lattice-based access control
B. Attribute-based access control
C. Rule-based access control
D. Discretionary access control

Answer: A,C

QUESTION NO: 60

You work as a Network Administrator for Net Perfect Inc. The company has a TCP/IP-based Windows NT network. You are configuring a computer that will be used as a file server on the network. You have to decide the disk configuration for the computer to obtain better performance.

A fault tolerant disk configuration is not a requirement. Which of the following RAID levels will you choose to fulfil the requirement?

A. RAID-1
B. RAID-5
C. RAID-4
D. RAID-3
E. RAID-0

Answer: E

QUESTION NO: 61

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: 62

Which of the following is also known as the 'Code for Information Security'?

A. ISO/IEC 20002 standard
B. ISO/IEC 27001:2005 standard
C. ISO/IEC 27002:2005 standard
D. ISO/IEC 20000 standard

Answer: C

QUESTION NO: 63

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You have been assigned the task to secure information labeling and handling within the organization. Which of the following controls of the ISO standard is concerned with information labeling and handling?

A. Control A.7.1.3
B. Control A.7.1.2
C. Control A.7.2.2
D. Control A.7.1.1

Answer: C

QUESTION NO: 64

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: 65

Which of the following documents is developed along the risk management processes to monitor

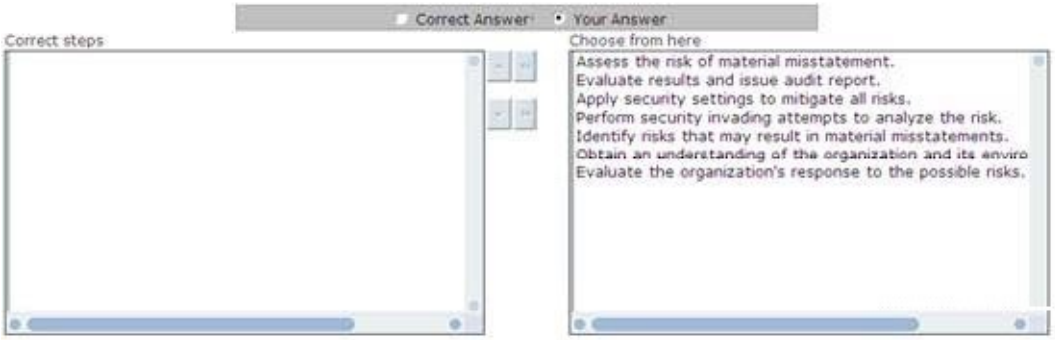
and control risks?

A. Fault tree
B. Risk mitigation
C. Decision tree
D. Risk register

Answer: D

QUESTION NO: 66

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



A.

Answer: A

QUESTION NO: 67

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: 68

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: 69

Which of the following is expressly set up to attract and trap people who attempt to penetrate other people's computer systems?

A. Honeypot
B. Internet bot
C. Crawler
D. Spider

Answer: A

QUESTION NO: 70

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: 71

Which of the following are the sub-elements of environmental security?

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

A. To prevent or respond to environmentally caused conflicts
B. To protect and assist environment from a material's potential
C. To prevent or repair military damage to the environment
D. To protect the environment due to its inherent moral value

Answer: A,C,D

QUESTION NO: 72

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: 73

Mark is hired as an Information Security Officer for BlueWell Inc. He wants to draw the attention of the management towards the significance of integrating information security in the business processes.

Which of the following tasks should he perform first to accomplish the task?

A. He should perform a risk assessment.
B. He should develop an information security policy.
C. He should set up a security budget.
D. He should obtain benchmarking information.

Answer: A

QUESTION NO: 74

You are working with a company that depends on real time data being available to employees, thus performance is an issue. They are trying to select the best method for handing the situation of a hard drive crashing. Which of the following would you recommend to them?

A. RAID 2
B. RAID 0
C. RAID 1
D. RAID 5

Answer: D

QUESTION NO: 75

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: 76

Sam is the CEO of Gentech Inc. The company is located in New York. He has to start a new project in order to increase the overall revenue of the company. Sam has to develop an ISMS policy. In which of the following phases of the PDCA cycle will Sam accomplish the task?

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

Answer: A

QUESTION NO: 77

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: 78

Which of the following controls help in the reduction of the effect of an attack?

A. Preventive controls
B. Directive controls
C. Corrective controls
D. Detective controls

Answer: C

QUESTION NO: 79

Which of the following statements is true about Return On Investment?

A. It is the difference between the benefit achieved and the amount spent to achieve that benefit; it is expressed as a percentage.
B. It is the extra value produced by establishment of benefits that include long-term outcomes. ROI is a sub-component of VOI.
C. It is the profit achieved through realization of improvements.
D. It is the outcome that is once compared to the earlier state, which shows a computable increase in a desirable metric or decrease in an undesirable metric.

Answer: A

QUESTION NO: 80

Which of the following federal laws are related to hacking activities?

Each correct answer represents a complete solution. Choose three.

A. 18 U.S.C. 1030
B. 18 U.S.C. 1028
C. 18 U.S.C. 1029
D. 18 U.S.C. 2510

Answer: A,C,D

QUESTION NO: 81

Which of the following provides secure online payment services?

A. ACH
B. ICSA
C. CA
D. IEEE

Answer: A

QUESTION NO: 82

Which of the following is a process of identifying and documenting project roles, responsibilities, and reporting relationships?

A. Capacity planning
B. Enterprise resource planning
C. Business Continuity planning
D. Human resource planning

Answer: D

QUESTION NO: 83

Which of the following is a list of specific actions being taken to deal with specific risks associated with the threats?

A. Risk transference
B. Risk avoidance
C. Risk acceptance
D. Risk mitigation

Answer: D

QUESTION NO: 84

Business Continuity Planning (BCP) determines the risks to the organizational processes and creates policies, plans, and procedures in order to minimize the impact of those risks. What are the different steps in the Business Continuity Planning process?

Each correct answer represents a part of the solution. Choose all that apply.

A. Business Analysis

B. Continuity planning
C. Project scope and planning
D. Approval and implementation
E. Business Impact Assessment

Answer: B,C,D,E

QUESTION NO: 85

Which of the following statements is correct about the Annual Loss Expectancy?

A. It is the size of the damage claims resulting from not having carried out risk analyses effec tively.
B. It is the average damage calculated by insurance companies for businesses in a country.
C. It is the minimum amount for which a company should insure itself.
D. It is the amount of damage that can occur as a result of an incident during the year.

Answer: D

QUESTION NO: 86

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: 87

John works as an IT Technician for uCertify Inc. One morning, John receives an e-mail from the company's Manager asking him to provide his logon ID and password, but the company policy

restricts users from disclosing their logon IDs and passwords. Which type of possible attack is this?

A. DoS
B. Trojan horse
C. Social engineering
D. Replay attack

Answer: C

QUESTION NO: 88

Sam works as a Network Administrator for Blue Well Inc. The company decides to opt for a strategy of a mix of measures to minimize risks. A stand-by arrangement is organized for the company. To which of the following categories of measures does a stand-by arrangement belong?

A. Corrective measures
B. Detective measures
C. Repressive measures
D. Preventive measures

Answer: C

QUESTION NO: 89

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: 90

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: 91

Mark works as a Software Developer for TechNet Inc. He has recently been fired, as he was caught doing some illegal work in the organization. Before leaving the organization, he decided to retaliate against the organization. He deleted some of the system files and made some changes in the registry files created by him. Which of the following types of attacks has Mark performed?

A. DDoS
B. Smurf
C. Logic bomb
D. Sabotage

Answer: C

QUESTION NO: 92

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: 93

Which of the following states that a user should never be given more privileges than are required to carry out a task?

A. Principle of least privilege
B. Role-based security
C. Security through obscurity
D. Segregation of duties

Answer: A

QUESTION NO: 94

Which of the following are the various types of risk analysis?

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

A. Corrective
B. Quantitative
C. Repressive
D. Qualitative

Answer: B,D

QUESTION NO: 95

Which of the following statements describes the purpose of information security policy?

A. The security policy makes the security plan flawless by providing the necessary details.
B. The security policy provides direction and support to the management regarding information

security.
C. Analysis of risks and search for countermeasures are known as Policy Documents.
D. The security policy provides details about threats and the consequences.

Answer: B

QUESTION NO: 96

Which of the following is the correct formula of single loss expectancy?

A. SLE= Annualized rate of occurrence*exposure factor
B. SLE=asset value*exposure factor
C. SLE= exposure factor*exposure factor
D. SLE= Annualized loss expectancy*exposure factor

Answer: B

QUESTION NO: 97

Which of the following statements are true about Information Security Management?

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

A. It is not designed to recognize, control, or protect information or any equipment that is used in connection with its processing.
B. It is designed to recognize, control, and protect information and any equipment that is used in connection with its storage and transmission.
C. Information Security is a system of policies and procedures.
D. Information Security Management has the objective to manage information security effectively within all service providers.

Answer: B,C,D

QUESTION NO: 98

Which of the following is the process of removing sensitive information from a document or any

other medium, so that it may be distributed to a broader audience?

A. Sanitization
B. Censorship
C. Pixelization
D. Data remanence

Answer: A

QUESTION NO: 99

You work as an Information Security Manager for uCertify Inc. You are working on asset management. You need to make a document on the usage of information assets. Which of the following controls of the ISO standard deals with the documentation and implementation of rules for the acceptable use of information assets?

A. Control A.7.2.1
B. Control A.7.1.2
C. Control A.7.1.3
D. Control A.7.2

Answer: D

QUESTION NO: 100

Which of the following is a formal state transition model of computer security policy that is used to describe a set of access control rules which use security labels on objects and clearances for subjects?

A. Five Pillars model
B. Classic information security model
C. Bell-LaPadula model
D. Clark-Wilson integrity model

Answer: C

QUESTION NO: 101

Mark works as a Network Security Administrator for uCertify Inc. He has installed IDS for matching incoming packets against known attacks. Which of the following types of intrusion detection techniques is being used?

A. Host-based IDS
B. Signature-based IDS
C. Pattern Matching IDS
D. Network-based IDS

Answer: C

QUESTION NO: 102

You work as a Security Professional for uCertify Inc. You have been assigned the task to calculate the Recovery Time Objective for particular outage duration. Which of the following should be included in the Recovery Time Objective?

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

A. Running applications back online
B. Recovering data
C. Fault detection
D. Sales estimation

Answer: A,B,C

QUESTION NO: 103

Which of the following are the basics of Business Continuity Management?

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

A. Identification of human resources according to the requirements
B. Regular checking of business continuity plans
C. Identification of authentication techniques according to the requirements
D. Implementation of a risk assessment technique to identify the causes and consequences of failures

Trying our product !

★ **100%** Guaranteed Success

★ **100%** Money Back Guarantee

★ **365 Days** Free Update

★ **Instant Download** After Purchase

★ **24x7** Customer Support

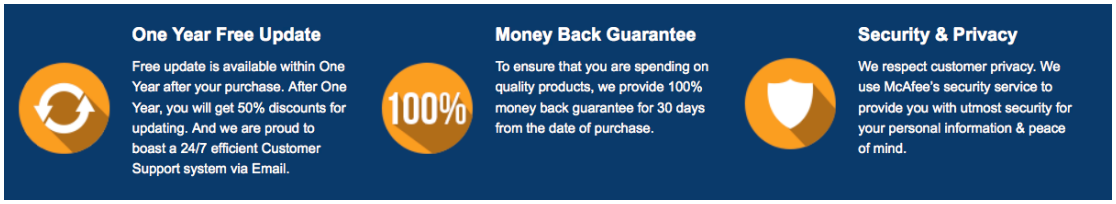
★ Average **99.9%** Success Rate

★ More than **69,000** Satisfied Customers Worldwide

★ Multi-Platform capabilities - **Windows, Mac, Android, iPhone, iPod, iPad, Kindle**

Need Help

Please provide as much detail as possible so we can best assist you.
To update a previously submitted ticket:



Guarantee & Policy | Privacy & Policy | Terms & Conditions