QUESTION 1101
Which of the following types of attack involves a program that creates an infinite loop, makes lots of copies of itself, and continues to open lots of files?

- **A. Local DoS attacks**
- B. Remote DoS attacks
- C. Distributed DoS attacks
- D. Local Virus attacks
- E. None of the choices

Answer: A
Topic: Local DoS Attacks
Explanation:
Local Denial-of-Service (DoS) attacks can involve a program that creates an infinite loop, makes copies of itself, and opens many files, ultimately overwhelming system resources. The best defense is to identify and terminate the malicious program.

QUESTION 1102
What is the best defense against Local DoS attacks?

- A. Patch your systems
- B. Run a virus checker
- C. Run anti-spyware software
- **D. Find this program and kill it**
- E. None of the choices

Answer: D
Topic: Local DoS Attacks
Explanation:
The best way to defend against Local DoS attacks is to identify and kill the malicious program causing the infinite loop and resource exhaustion. While other security measures are important, killing the offending program is the immediate solution.

QUESTION 1103
Which of the following are examples of tools for launching Distributed DoS Attacks (choose all that apply):

- **TFN**
- **TFN2K**
- **Trin00**
- **Stacheldracht**
- Tripwire

Answer: A, B, C, D
Topic: Distributed DoS Tools
Explanation:
Tools such as TFN, TFN2K, Trin00, and Stacheldracht are commonly used for Distributed Denial-of-Service (DDoS) attacks. These attacks involve coordinating multiple compromised systems to send malicious packets. The best defense includes system patching and appropriate firewall configurations.

QUESTION 1104
What is the best defense against Distributed DoS Attack?

- **A. Patch your systems**
- B. Run a virus checker
- C. Run anti-spyware software
- D. Find the DoS program and kill it
- E. None of the choices

Answer: A
Topic: Defense Against DDoS
Explanation:
The best defense against Distributed DoS attacks is to ensure that all systems are patched and up-to-date, and that firewalls are properly configured to block malicious traffic. These measures help to mitigate the impact of such attacks.

QUESTION 1105
What is wrong with a Black Box type of intrusion detection system?

- A. You cannot patch it
- B. You cannot test it
- **C. You cannot examine its internal workings from outside**
- D. You cannot tune it
- E. None of the choices

Answer: C
Topic: Black Box IDS
Explanation:
A Black Box intrusion detection system (IDS) is one where the internal workings are not visible to external users. This lack of transparency can make it difficult to evaluate its effectiveness, troubleshoot issues, or fine-tune its performance.

QUESTION 1106
Which of the following are often considered as the first defensive line in protecting a typical data and information environment?

- Certificates
- Security token
- **Password**
- Biometrics
- E. None of the choices

Answer: C
Topic: First Line of Defense
Explanation:
Passwords are generally considered the first line of defense in protecting data and information. Users need to understand the importance of strong passwords and how they contribute to security.

QUESTION 1107
Which of the following are the characteristics of a good password?

- **A. It has mixed-case alphabetic characters, numbers, and symbols**
- B. It has mixed-case alphabetic characters and numbers
- C. It has mixed-case alphabetic characters and symbols
- D. It has mixed-case alphabetic characters, numbers, and binary codes
- E. None of the choices

Answer: A
Topic: Characteristics of Good Passwords
Explanation:
A good password should include mixed-case alphabetic characters, numbers, and symbols. This combination increases the complexity and makes it harder to guess or crack the password.

QUESTION 1108
What is the recommended minimum length of a good password?

- A. 6 characters
- **B. 8 characters**
- C. 12 characters

- D. 18 characters
- E. 22 characters
- F. None of the choices

Answer: B
Topic: Password Length
Explanation:
A good password should have at least 8 characters to provide adequate protection. Longer passwords are better, but 8 characters is generally considered the minimum for effective security.

QUESTION 1109
Which of the following is a good tool to use to help enforce the deployment of good passwords?

- A. Password cracker
- B. Local DoS attacker
- C. Network hacker
- D. Remote windowing tool
- E. None of the choices

Answer: A
Topic: Enforcing Good Password Practices
Explanation:
A password cracker tool can be used to test the strength of passwords and identify weak ones. It is a useful tool to periodically check and enforce good password practices, requiring users to change easily cracked passwords.

QUESTION 1110
Which of the following is a good time frame for making changes to passwords?

- A. Every 180 to 365 days
- B. Every 30 to 45 days
- C. Every 10 to 20 days
- **D. Every 90 to 120 days**
- E. None of the choices

Answer: D
Topic: Password Change Frequency
Explanation:
It is recommended to change passwords every 90 to 120 days. This helps to ensure that compromised passwords are quickly replaced, improving overall security.

QUESTION 1111
You should keep all computer rooms at reasonable temperatures, which is in between (choose all that apply):

- **A. 60 - 75 degrees Fahrenheit**
- **B. 10 - 25 degrees Celsius**
- C. 30 - 45 degrees Fahrenheit
- D. 1 - 15 degrees Celsius
- E. 20 - 35 degrees Fahrenheit
- F. 0 - 5 degrees Celsius

Answer: A, B
Explanation:
Computer rooms should be kept at temperatures between 60 - 75 degrees Fahrenheit or 10 - 25 degrees Celsius to ensure proper functioning of the hardware. Additionally, humidity levels should be maintained between 20 - 70 percent.

QUESTION 1112
You should keep all computer rooms at reasonable humidity levels, which are in between:

- **A. 20 - 70 percent**
- B. 10 - 70 percent
- C. 10 - 60 percent
- D. 70 - 90 percent
- E. 60 - 80 percent
- F. None of the choices

Answer: A
Explanation:
Humidity levels in computer rooms should be kept between 20 - 70 percent. This helps prevent static electricity and condensation, which could damage sensitive equipment.

QUESTION 1113
A virus typically consists of what major parts (choose all that apply):

- **A. A mechanism that allows them to infect other files and reproduce, a trigger that activates delivery of a "payload"**
- **B. A payload**
- **C. A signature**
- D. None of the choices

Answer: A, B, C
Explanation:
A typical virus consists of three main parts:

- A mechanism to infect files and reproduce,
- A trigger to activate the delivery of the payload,
- A payload that carries out the malicious action.
  The signature is used to identify the virus, but it's not considered part of the virus itself.

QUESTION 1114
Within a virus, which component is responsible for what the virus does to the victim file?

- **A. The payload**
- B. The signature
- C. The trigger
- D. The premium
- E. None of the choices

Answer: A
Explanation:
The payload is the part of the virus responsible for executing its malicious actions on the victim file, which is typically the most destructive part of the virus.

QUESTION 1115
Which of the following can be thought of as the simplest and almost cheapest type of firewall?

- A. Stateful firewall
- B. Hardware firewall
- C. PIX firewall
- **D. Packet filter**
- E. None of the choices

Answer: D
Explanation:
A packet filter firewall is the simplest and cheapest type of firewall. It filters traffic based on packet information, such as IP address and port, without maintaining state information.

QUESTION 1116
Screening router inspects traffic through examining:

- **A. Message header**

- B. Virus payload
- C. Message content
- D. Attachment type
- E. None of the choices

Answer: A
Explanation:
A screening router inspects network traffic by analyzing the message header, which contains key information such as the source and destination IP addresses and port numbers.

QUESTION 1117
A major portion of what is required to address nonrepudiation is accomplished through the use of:

- A. Strong methods for authentication and ensuring data validity
- **B. Strong methods for authentication and ensuring data integrity**
- C. Strong methods for authorization and ensuring data integrity
- D. Strong methods for authentication and ensuring data reliability
- E. None of the choices

Answer: B
Explanation:
Nonrepudiation is primarily achieved through strong authentication methods (verifying the identity of users) and ensuring data integrity (ensuring the data has not been tampered with), preventing parties from denying their actions.

QUESTION 1118
Why is it not preferable for a firewall to treat each network frame or packet in isolation?

- **A. Such a firewall has no way of knowing if any given packet is part of an existing connection, is trying to establish a new connection, or is just a rogue packet.**
- B. Such a firewall is costly to set up.
- C. Such a firewall is too complicated to maintain.
- D. Such a firewall is CPU hungry.
- E. Such a firewall offers poor compatibility.
- F. None of the choices

Answer: A
Explanation:
A stateless firewall treats each packet in isolation, which makes it difficult to determine the context of a packet (whether it's part of an ongoing session, a new connection, or potentially malicious). This lack of context can lead to security issues.

QUESTION 1119
Phishing attack works primarily through:

- **A. Email and hyperlinks**
- B. SMS
- C. Chat
- D. Email attachment
- E. News
- F. File download
- G. None of the choices

Answer: A
Explanation:
Phishing attacks typically work through email and hyperlinks. Attackers send emails that appear to come from legitimate sources, containing links to fraudulent websites designed to steal sensitive information.

QUESTION 1120
Which of the following types of attack often take advantage of curiosity or greed to deliver malware?

- **A. Gimmes**
- B. Tripwire
- C. Icing
- D. Soft coding
- E. Pretexting
- F. None of the choices

Answer: A
Explanation:
Gimmes, also known as Trojan Horses, take advantage of curiosity or greed to deliver malware. They often arrive as email attachments that promise something desirable, and users may be tricked into opening them, allowing the malware to be executed.

QUESTION 1121
Gimmes often work through:
- A. SMS
- B. IRC chat
- **C. Email attachment**
- D. News
- E. File download
- F. None of the choices

Answer: C
Explanation:
Gimmes, also known as Trojan Horses, take advantage of curiosity or greed to deliver malware. They often arrive as email attachments, promising something enticing, and trick the recipient into opening them, which leads to the execution of malware.

QUESTION 1122
Talking about biometric authentication, physical characteristics typically include (choose all that apply):
- **A. Fingerprints**
- **B. Eye retinas**
- **C. Irises**
- **D. Facial patterns**
- **E. Hand measurements**
- F. None of the choices

Answer: A, B, C, D, E
Explanation:
Biometric authentication involves using physical and behavioral characteristics for authentication. Physical characteristics include fingerprints, eye retinas, irises, facial patterns, and hand measurements.

QUESTION 1123
Talking about biometric authentication, which of the following is often considered as a mix of both physical and behavioral characteristics?
- **A. Voice**
- B. Finger measurement
- C. Body measurement
- D. Signature
- E. None of the choices

Answer: A
Explanation:
Voice is considered a mix of both physical and behavioral characteristics in biometric authentication. It involves physical attributes (the sound of the voice) and behavioral aspects (speech patterns).

QUESTION 1124
Performance of a biometric measure is usually referred to in terms of (choose all that apply):
- A. Failure to reject rate
- **B. False accept rate**
- **C. False reject rate**
- **D. Failure to enroll rate**
- E. None of the choices

Answer: B, C, D
Explanation:
The performance of a biometric system is commonly measured using:
- False accept rate (FAR) — the rate at which invalid users are accepted,
- False reject rate (FRR) — the rate at which valid users are rejected,
- Failure to enroll rate (FER) — the rate at which users fail to enroll in the system.

QUESTION 1125
Talking about biometric measurement, which of the following measures the percent of invalid users who are incorrectly accepted in?
- A. Failure to reject rate
- **B. False accept rate**
- C. False reject rate
- D. Failure to enroll rate
- E. None of the choices

Answer: B
Explanation:
The False Accept Rate (FAR) measures the percentage of invalid users who are incorrectly accepted by the biometric system.

QUESTION 1126
An accurate biometric system usually exhibits (choose all that apply):
- **A. Low EER**
- **B. Low CER**
- C. High EER
- D. High CER
- E. None of the choices

Answer: A, B
Explanation:
An accurate biometric system typically has a low Equal Error Rate (EER) and low Cross-over Error Rate (CER), which indicates that the rates of both false acceptances and false rejections are minimal and balanced.

QUESTION 1127
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses which stream cipher for confidentiality?
- A. CRC-32
- B. CRC-64
- C. DES
- D. 3DES
- **E. RC4**
- F. RC5
- G. None of the choices

Answer: E
Explanation:

Wired Equivalent Privacy (WEP), part of the IEEE 802.11 standard, uses the RC4 stream cipher for ensuring confidentiality in wireless networks.

QUESTION 1128
As part of the IEEE 802.11 standard ratified in September 1999, WEP uses the CRC-32 checksum for:

- **A. Integrity**
- B. Validity
- C. Accuracy
- D. Confidentiality
- E. None of the choices

Answer: A
Explanation:
WEP uses the CRC-32 checksum for integrity, ensuring that data has not been tampered with during transmission.

QUESTION 1129
Many WEP systems require a key in a relatively insecure format. What format is this?

- A. Binary format
- **B. Hexadecimal format**
- C. 128 bit format
- D. 256 bit format
- E. None of the choices

Answer: B
Explanation:
Many WEP systems require keys in hexadecimal format, which can be insecure because easily guessable words can be selected in the limited hex character set (0-9, A-F).

QUESTION 1130
Wi-Fi Protected Access implements the majority of which IEEE standard?

- **A. 802.11i**
- B. 802.11g
- C. 802.11x
- D. 802.11v
- E. None of the choices

Answer: A
Explanation:
Wi-Fi Protected Access (WPA) implements the majority of the IEEE 802.11i standard, which provides enhanced security for wireless networks.

QUESTION 1131
One major improvement in WPA over WEP is the use of a protocol which dynamically changes keys as the system is used. What protocol is this?

- A. SKIP
- B. RKIP
- C. OKIP
- D. EKIP
- **E. TKIP**
- F. None of the choices

Answer: E
Explanation:
Temporal Key Integrity Protocol (TKIP) is a major improvement in WPA over WEP. It dynamically changes keys as the system is used, improving security.

QUESTION 1132
Which of the following refers to a symmetric key cipher which operates on fixed-length groups of bits with an unvarying transformation?

- A. Stream cipher
- **B. Block cipher**
- C. Check cipher
- D. String cipher
- E. None of the choices

Answer: B
Explanation:
A block cipher is a symmetric key cipher that operates on fixed-length blocks of data and applies the same transformation to each block. This is in contrast to stream ciphers, which encrypt data one bit or byte at a time.

QUESTION 1133
Which of the following typically consists of a computer, some real looking data and/or a network site that appears to be part of a production network but which is in fact isolated and well prepared?

- **A. Honeypot**
- B. Superpot
- C. IDS
- D. IPS
- E. Firewall
- F. None of the choices

Answer: A
Explanation:
A honeypot is a security resource that appears to be part of a legitimate network but is actually a decoy used to attract and trap attackers, allowing security teams to detect and analyze unauthorized activity.
Q1134
Which of the following is a tool you can use to simulate a big network structure on a single computer?

- honeymoon
- honeytrap
- honeytube
- honeyd
- None of the choices.

Answer: D
Explanation:
honeyd is a GPL licensed software you can use to simulate a big network structure on a single computer.
Topic: Network Simulation Tools

QUESTION 1135
Which of the following are valid choices for the Apache/SSL combination (choose all that apply):

- the Apache-SSL project
- third-party SSL patches
- the mod_ssl module
- the mod_css module
- None of the choices.

Answer: A,B,C
Explanation:
On Linux, Apache is a safer choice of web service. Several options are available for the Apache/SSL combination, such as the Apache-SSL using third-party SSL patches, or compiling Apache with the mod_ssl module.
Topic: SSL Configurations for Apache

QUESTION 1136
What would be the major purpose of a rootkit?
- A. to hide evidence from system administrators.
- B. to encrypt files for system administrators.
- C. to corrupt files for system administrators.
- D. to hijack system sessions.
- E. None of the choices.

Answer: A
Explanation:
A rootkit is designed to hide evidence of intrusions or malicious activities from system administrators, making it difficult to detect unauthorized access attempts.
Topic: Rootkits and Malicious Software

QUESTION 1137
Most trojan horse programs are spread through:
- e-mails.
- MP3.
- MS Office.
- Word template.
- None of the choices.

Answer: A
Explanation:
Most trojan horse programs are spread through e-mails. Some earlier trojan horse programs were bundled in "Root Kits". For example, the Linux Root Kit version 3 (lrk3) released in December 96 included tcp wrapper trojans. Portable Linux devices can also be affected by trojan horses.
Topic: Trojan Horse and Malware Distribution

QUESTION 1138
The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?
- e-mails.
- MP3.
- MS Office.
- Word template.
- None of the choices.

Answer: B
Explanation:
The Trojan.Linux.JBellz Trojan horse runs as a malformed .mp3 file.
Topic: Malformed File Formats in Trojan Attacks

QUESTION 1139
Which of the following types of spyware was originally designed for determining the sources of error or for measuring staff productivity?
- A. Keywords logging
- B. Keystroke logging
- C. Directory logging
- D. Password logging
- E. None of the choices.

Answer: B
Explanation:
Keystroke logging (in the form of spyware) was initially a diagnostic tool deployed by software developers to capture user keystrokes and determine sources of error or measure productivity.
Topic: Keystroke Logging and Spyware

QUESTION 1140
You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?
- exploit
- vulnerability
- both

Answer: B
Explanation:
An exploit refers to software or commands that take advantage of a bug or vulnerability in order to cause unintended behavior. A vulnerability refers to a weakness in the system itself.
Topic: Exploits vs Vulnerabilities

QUESTION 1141
Which of the following is a rewrite of ipfwadm?
- ipchains
- iptables
- Netfilter
- ipcook
- None of the choices.

Answer: A
Explanation:
ipchains is a rewrite of ipfwadm, used on earlier Linux systems. It is superseded by iptables in Linux 2.4 and above. Iptables is based on the Netfilter framework.
Topic: Linux Firewall Systems

QUESTION 1142
Iptables is based on which of the following frameworks?
- Netfilter
- NetDoom
- NetCheck
- NetSecure
- None of the choices.

Answer: A
Explanation:
Iptables is based on the Netfilter framework, which provides hooks within the Linux kernel to intercept and manipulate network packets.
Topic: Netfilter and Iptables

QUESTION 1143
Cisco IOS based routers perform basic traffic filtering via which of the following mechanisms?
- A. datagram scanning
- B. access lists
- C. stateful inspection
- D. state checking
- E. link progressing
- F. None of the choices.

Answer: B
Explanation:
On Cisco IOS-based routers, you can use access lists (ACLs) to perform basic traffic filtering, controlling network traffic flow based on predefined rules.
Topic: Cisco IOS ACLs and Traffic Filtering

QUESTION 1144
Which of the following correctly describe the potential problem of deploying Wi-Fi Protected Access to secure your wireless network?

- A. potential compatibility problems with wireless network interface cards.
- B. potential compatibility problems with wireless access points.
- C. potential performance problems with wireless network interface cards.
- D. potential performance problems with wireless access points.
- E. None of the choices.

Answer: B
Explanation:
Wi-Fi Protected Access (WPA/WPA2) may encounter compatibility problems with first-generation wireless access points.
Topic: Wi-Fi Protected Access (WPA/WPA2) Compatibility Issues

---

QUESTION 1145
The Federal Information Processing Standards (FIPS) were developed by:

- A. the United States Federal government
- B. ANSI
- C. ISO
- D. IEEE
- E. IANA
- F. None of the choices.

Answer: A
Explanation:
FIPS are standards developed by the United States Federal government for use by all non-military government agencies and contractors.
Topic: Federal Information Processing Standards (FIPS)

QUESTION 1146
The Federal Information Processing Standards (FIPS) are primarily for use by (choose all that apply):

- all non-military government agencies
- US government contractors
- all military government agencies
- all private and public colleges in the US
- None of the choices.

Answer: A, B
Explanation:
FIPS are primarily for use by non-military government agencies and US government contractors. They may also modify versions of community standards.
Topic: FIPS Usage and Application

QUESTION 1147
Sophisticated database systems provide many layers and types of security, including (choose all that apply):

- A. Access control
- B. Auditing
- C. Encryption
- D. Integrity controls
- E. Compression controls

Answer: A, B, C, D
Explanation:
Sophisticated database systems offer various security layers, including access control, auditing,

encryption, and integrity controls. Vulnerability assessments are essential to identify misconfigurations or weaknesses.
Topic: Database Security Layers

QUESTION 1148
Which of the following refers to an important procedure when evaluating database security (choose the BEST answer)?

- A. performing vulnerability assessments against the database.
- B. performing data check against the database.
- C. performing dictionary check against the database.
- D. performing capacity check against the database system.
- E. None of the choices.

Answer: A
Explanation:
Performing vulnerability assessments against the database is essential when evaluating database security to identify misconfigurations and vulnerabilities.
Topic: Vulnerability Assessment for Database Security

QUESTION 1149
Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

- Strong-factor authentication
- Two-factor authentication
- Dual-password authentication
- Two-passphrases authentication
- Dual-keys authentication
- Rich-factor authentication

Answer: B
Explanation:
Two-factor authentication requires two independent methods to verify identity and privileges. This often involves "something you know" and "something you have" or "something you are."
Topic: Two-Factor Authentication

QUESTION 1150
Common implementations of strong authentication may use which of the following factors in their authentication efforts (choose all that apply):

- A. 'something you know'
- B. 'something you have'
- C. 'something you are'
- D. 'something you have done in the past on this same system'
- E. 'something you have installed on this same system'
- F. None of the choices.

Answer: A, B, C
Explanation:
Common factors in strong authentication include "something you know" (e.g., a password), "something you have" (e.g., a token), and "something you are" (e.g., biometrics). Using more than one factor provides stronger authentication.
Topic: Strong Authentication Factors

QUESTION 1151
Effective transactional controls are often capable of offering which of the following benefits (choose all that apply):

- A. reduced administrative and material costs

- B. shortened contract cycle times
- C. enhanced procurement decisions
- D. diminished legal risk
- E. None of the choices

Answer: A, B, C, D
Explanation:
Transactional systems provide a baseline necessary to measure and monitor contract performance and provide a method for appraising efficiency against possible areas of exposure. Effective transactional controls reduce administrative and material costs, shorten contract cycle times, enhance procurement decisions, and diminish legal risk.
Topic: Transactional Controls and Business Efficiency

QUESTION 1152
In the context of physical access control, what is known as the process of verifying user identities?

- Authentication
- Authorization
- Accounting
- Encryption
- Compression
- None of the choices

Answer: A
Explanation:
Authentication is the process of verifying a user's claimed identity. It is based on at least one of these three factors: Something you know, Something you have, or Something you are.
Topic: Physical Access Control and Authentication

QUESTION 1153
Physical access controls are usually implemented based on which of the following means (choose all that apply):

- A. mechanical locks
- B. guards
- C. operating systems
- D. transaction applications
- E. None of the choices

Answer: A, B
Explanation:
In physical security, access control refers to the practice of restricting entrance to authorized persons. Human means of enforcement include guards, receptionists, etc. Mechanical means may include locks and keys.
Topic: Physical Security and Access Control

QUESTION 1154
Fault-tolerance is a feature particularly sought-after in which of the following kinds of computer systems (choose all that apply):

- A. desktop systems
- B. laptop systems
- C. handheld PDAs
- D. business-critical systems
- E. None of the choices

Answer: D
Explanation:
Fault-tolerance enables a system to continue operating properly in the event of the failure of some parts

of it. It avoids total breakdown, and is particularly sought-after in high-availability environments full of business-critical systems.
Topic: Fault-Tolerance and Business Continuity

QUESTION 1155
The technique of rummaging through commercial trash to collect useful business information is known as:

- A. Information diving
- B. Intelligence diving
- C. Identity diving
- D. System diving
- E. Program diving
- F. None of the choices

Answer: A
Explanation:
Dumpster diving (also known as information diving) is the practice of rummaging through commercial trash to find useful information such as files, letters, memos, passwords, etc.
Topic: Social Engineering and Information Gathering

QUESTION 1156
Which of the following refers to a primary component of corporate risk management with the goal of minimizing the risk of prosecution for software piracy due to use of unlicensed software?

- A. Software audit
- B. System audit
- C. Application System audit
- D. Test audit
- E. Mainframe audit
- F. None of the choices

Answer: A
Explanation:
Software audits are a component of corporate risk management, aimed at minimizing the risk of prosecution for software piracy due to the use of unlicensed software.
Topic: Software Audits and Risk Management

QUESTION 1157
The purpose of a mainframe audit is to provide assurance that (choose all that apply):

- A. processes are being implemented as required
- B. the mainframe is operating as it should
- C. security is strong
- D. procedures in place are working
- E. procedures in place are updated as needed
- F. the OS applications are secured
- G. None of the choices

Answer: A, B, C, D, E
Explanation:
The purpose of a mainframe audit is to provide assurance that processes are being implemented as required, the mainframe is operating as it should, security is strong, and that procedures in place are working and are updated as needed.
Topic: Mainframe Audits and Assurance

QUESTION 1158
In a security server audit, focus should be placed on (choose all that apply):

- A. proper segregation of duties

- B. adequate user training
- C. continuous and accurate audit trail
- D. proper application licensing
- E. system stability
- F. performance and controls of the system
- G. None of the choices

Answer: A, C
Explanation:
Security server audits should focus on ensuring proper segregation of duties and a continuous and accurate audit trail, ensuring that security administrators' roles and privileges are properly controlled.
Topic: Security Server Audits and Control

QUESTION 1159
Talking about application system audit, focus should always be placed on:
- A. performance and controls of the system
- B. the ability to limit unauthorized access and manipulation
- C. input of data are processed correctly
- D. output of data are processed correctly
- E. changes to the system are properly authorized
- F. None of the choices

Answer: A, B, C, D, E
Explanation:
For application system audits, the focus should be on system performance, access control, proper data input and output processing, and ensuring that system changes are authorized.
Topic: Application System Audits and Controls

QUESTION 1160
A successful risk-based IT audit program should be based on:
- A. an effective scoring system.
- B. an effective PERT diagram.
- C. an effective departmental brainstorm session.
- D. an effective organization-wide brainstorm session.
- E. an effective yearly budget.
- F. None of the choices

Answer: A
Explanation:
A successful risk-based IT audit program should be based on an effective scoring system, considering all relevant risk factors to prioritize audit resources.
Topic: Risk-Based IT Audit Programs

QUESTION 1161
The use of risk assessment tools for classifying risk factors should be formalized in your IT audit effort through:
- A. the use of risk controls.
- B. the use of computer assisted functions.
- C. using computer assisted audit technology tools.
- D. the development of written guidelines.
- E. None of the choices

Answer: D
Explanation:
Risk assessment tools should be formalized in IT audits through the development of written guidelines on their use, which helps ensure objectivity in evaluating risk factors.
Topic: Risk Assessment Tools in IT Audits

QUESTION 1162
Which of the following correctly describes the purpose of an Electronic data processing audit?

- A. to collect and evaluate evidence of an organization's information systems, practices, and operations.
- B. to ensure document validity.
- C. to verify data accuracy.
- D. to collect and evaluate benefits brought by an organization's information systems to its bottomline.
- E. None of the choices

Answer: A
Explanation:
An Electronic Data Processing (EDP) audit is an IT audit process focused on collecting and evaluating evidence of an organization's information systems, practices, and operations.
Topic: Electronic Data Processing (EDP) Audits

QUESTION 1163
What should be done to determine the appropriate level of audit coverage for an organization's IT environment?

- A. determine the company's quarterly budget requirement.
- B. define an effective assessment methodology.
- C. calculate the company's yearly budget requirement.
- D. define an effective system upgrade methodology.
- E. define an effective network implementation methodology.

Answer: B
Explanation:
To determine the appropriate level of audit coverage, it is essential to define an effective assessment methodology and prioritize audit resources accordingly.
Topic: Determining Audit Coverage in IT Environments

QUESTION 1164
IS audits should be selected through a risk analysis process to concentrate on:

- A. those areas of greatest risk and opportunity for improvements.
- B. those areas of least risk and opportunity for improvements.
- C. those areas of the greatest financial value.
- D. areas led by the key people of the organization.
- E. random events.
- F. irregular events.

Answer: A
Explanation:
IS audits should focus on areas of greatest risk and potential for improvements, concentrating resources where they will have the most significant impact.
Topic: Risk Analysis in IS Audits

QUESTION 1165
Your final audit report should be issued:

- A. after an agreement on the observations is reached.
- B. before an agreement on the observations is reached.
- C. if an agreement on the observations cannot be reached.
- D. without mentioning the observations.
- E. None of the choices

Answer: A

Explanation:
The final audit report should be issued after an agreement is reached on the observations between the audit team and management.
Topic: Finalizing Audit Reports

QUESTION 1166
Well-written risk assessment guidelines for IS auditing should specify which of the following elements at the least (choose all that apply):

- A. A maximum length for audit cycles.
- B. The timing of risk assessments.
- C. Documentation requirements.
- D. Guidelines for handling special cases.
- E. None of the choices

Answer: A, B, C, D
Explanation:
A well-written risk assessment guideline should specify a maximum length for audit cycles, the timing of risk assessments, documentation requirements, and guidelines for handling special cases. These elements ensure a structured and effective risk management process.
Topic: Risk Assessment Guidelines in IS Auditing

QUESTION 1167
The ability of the internal IS audit function to achieve desired objectives depends largely on:

- A. the training of audit personnel
- B. the background of audit personnel
- C. the independence of audit personnel
- D. the performance of audit personnel
- E. None of the choices

Answer: C
Explanation:
The ability of the internal IS audit function to achieve desired objectives depends largely on the independence of audit personnel. The audit function should be free from conflicts of interest to perform its duties effectively.
Topic: Independence in IS Auditing

QUESTION 1168
In-house personnel performing IS audits should possess which of the following knowledge and/or skills (choose 2):

- A. information systems knowledge commensurate with the scope of the IT environment in question
- B. sufficient analytical skills to determine root cause of deficiencies in question
- C. sufficient knowledge on secure system coding
- D. sufficient knowledge on secure platform development
- E. information systems knowledge commensurate outside of the scope of the IT environment in question

Answer: A, B
Explanation:
Personnel performing IS audits should have information systems knowledge appropriate to the scope of the IT environment and sufficient analytical skills to determine the root cause of deficiencies.
Topic: Skills and Knowledge for IS Auditors

QUESTION 1169
A comprehensive IS audit policy should include guidelines detailing what involvement the internal audit team should have?

- A. in the development and coding of major OS applications.
- B. in the acquisition and maintenance of major WEB applications.
- C. in the human resource management cycle of the application development project.
- D. in the development, acquisition, conversion, and testing of major applications.
- E. None of the choices

Answer: D
Explanation:
An IS audit policy should outline the involvement of the internal audit team in the development, acquisition, conversion, and testing of major applications. This ensures that the audit team can evaluate the integrity and security of new systems.
Topic: Internal Audit Involvement in Application Development

QUESTION 1170
For application acquisitions with significant impacts, participation of your IS audit team should be encouraged:
- A. early in the due diligence stage.
- B. at the testing stage.
- C. at the final approval stage.
- D. at the budget preparation stage.
- E. None of the choices

Answer: A
Explanation:
For acquisitions with significant IT impacts, the IS audit team should be involved early in the due diligence stage to assess potential risks and ensure that the acquisition aligns with the organization's goals and security standards.
Topic: IS Audit Participation in Application Acquisitions

QUESTION 1171
Which of the following should be seen as one of the most significant factors considered when determining the frequency of IS audits within your organization?
- A. The cost of risk analysis
- B. The income generated by the business function
- C. Resource allocation strategy
- D. The nature and level of risk
- E. None of the choices

Answer: D
Explanation:
The nature and level of risk should be the most significant factors to be considered when determining the frequency of IS audits. Risk assessments should be updated regularly to reflect any changes in the business environment, and audits should focus on areas of higher risk.
Topic: Risk-Based Frequency of IS Audits

QUESTION 1172
Properly planned risk-based audit programs are often capable of offering which of the following benefits?
- A. audit efficiency and effectiveness.
- B. audit efficiency only.
- C. audit effectiveness only.
- D. audit transparency only.
- E. audit transparency and effectiveness.
- F. None of the choices

Answer: A

Explanation:
Risk-based audit programs enhance both audit efficiency and effectiveness. These programs allow auditors to focus on the most critical areas, improving overall audit outcomes.
Topic: Benefits of Risk-Based Audit Programs

QUESTION 1173
The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- the target's management hands-on involvement.
- the target's location.
- the target's size and complexity.
- the target's budget.
- the target's head count.
- None of the choices

Answer: C
Explanation:
The sophistication and formality of IS audit programs vary significantly depending on the size and complexity of the organization. Larger, more complex organizations require more formal and detailed audit programs.
Topic: Factors Influencing IS Audit Program Sophistication

QUESTION 1174
Which of the following is one of the most common ways that spyware is distributed?

- A. as a trojan horse.
- B. as a virus.
- C. as an Adware.
- D. as a device driver.
- E. as a macro.
- F. None of the choices

Answer: A
Explanation:
Spyware is often distributed as a Trojan horse. It is typically bundled with legitimate software that users download, and once installed, the spyware runs secretly alongside the desired software.
Topic: Methods of Spyware Distribution

QUESTION 1175
Which of the following is not a good tactic to use against hackers?

- A. Enticement
- B. Entrapment

Answer: B
Explanation:
Enticement occurs after someone has gained unlawful access to a system and lures them to a controlled environment like a "honey pot." Entrapment, on the other hand, involves encouraging someone to commit unlawful access, which is considered an unethical tactic.
Topic: Tactics Against Hackers

QUESTION 1176
Creating which of the following is how a hacker can ensure his ability to return to the hacked system at will?

- A. rootsec
- B. checksum
- C. CRC
- D. backdoors

- E. None of the choices

Answer: D
Explanation:
A backdoor is an undocumented method of accessing a system, often used by hackers to maintain access to compromised systems for later use. These can be used to bypass standard security measures.
Topic: Backdoors in Hacking

QUESTION 1177
A trojan horse simply cannot operate autonomously.
- true
- false

Answer: A
Explanation:
A Trojan horse cannot operate autonomously. It requires user interaction to trigger the malicious payload. For example, a user must run a seemingly harmless program for the Trojan to activate.
Topic: Characteristics of Trojan Horses

QUESTION 1178
Which of the following refers to the collection of policies and procedures for implementing controls capable of restricting access to computer software and data files?
- A. Binary access control
- B. System-level access control
- C. Logical access control
- D. Physical access control
- E. Component access control
- F. None of the choices

Answer: C
Explanation:
Logical access control refers to the use of policies, procedures, and controls to manage access to software and data files, ensuring that only authorized users can access sensitive information.
Topic: Logical Access Control

QUESTION 1179
A live test of a mutual agreement for IT system recovery has been carried out, including a four-hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:
- system and the IT operations team can sustain operations in the emergency environment.
- resources and the environment could sustain the transaction load.
- connectivity to the applications at the remote site meets response time requirements.
- workflow of actual business operations can use the emergency system in case of a disaster.

Correct Answer: A
Topic: Disaster Recovery Testing
Explanation: The test primarily checks the system's and the IT operations team’s ability to handle operations in an emergency. While transaction loads and connectivity are tested, the actual capacity of the system and team to handle full operations (including ancillary tasks) is only partially assessed.

QUESTION 1180
To address an organization's disaster recovery requirements, backup intervals should not exceed the:
- service level objective (SLO).
- recovery time objective (RTO).
- recovery point objective (RPO).
- maximum acceptable outage (MAO).

Correct Answer: C
Topic: Data Backup and Recovery Objectives
Explanation: The recovery point objective (RPO) defines how much data loss is acceptable, and backup intervals should not exceed this objective. Backups should ensure that data is restored to this point after a disaster.

QUESTION 1181
Which of the following would have the HIGHEST priority in a business continuity plan (BCP)?
- Resuming critical processes
- Recovering sensitive processes
- Restoring the site
- Relocating operations to an alternative site

Correct Answer: A
Topic: Prioritization in Business Continuity Planning
Explanation: The highest priority in a BCP is resuming critical business processes as soon as possible after a disruption to minimize operational impact.

QUESTION 1182
After completing the business impact analysis (BIA), what is the next step in the business continuity planning process?
- Test and maintain the plan.
- Develop a specific plan.
- Develop recovery strategies.
- Implement the plan.

Correct Answer: C
Topic: Business Continuity Planning Process
Explanation: After the Business Impact Analysis (BIA), the next step is to develop recovery strategies, which guide the recovery of the critical processes identified in the BIA.

QUESTION 1183
Which of the following is an appropriate test method to apply to a business continuity plan (BCP)?
- Pilot
- Paper
- Unit
- System

Correct Answer: B
Topic: Business Continuity Plan Testing
Explanation: A paper test, also known as a walk-through, involves reviewing the plan with key stakeholders to identify potential issues in a simulated disaster scenario without using actual resources.

QUESTION 1184
An IS auditor has audited a business continuity plan (BCP). Which of the following findings is the MOST critical?
- Nonavailability of an alternate private branch exchange (PBX) system
- Absence of a backup for the network backbone
- Lack of backup systems for the users' PCs
- Failure of the access card system

Correct Answer: B
Topic: Critical Infrastructure for Business Continuity
Explanation: A network backbone is critical for all network communications, and its failure would have the most severe impact. A PBX system failure or backup for PCs, while significant, would not cause as much disruption as the loss of the entire network.

QUESTION 1185
As part of the business continuity planning process, which of the following should be identified FIRST in the business impact analysis?
- Organizational risks, such as single point-of-failure and infrastructure risk
- Threats to critical business processes
- Critical business processes for ascertaining the priority for recovery
- Resources required for resumption of business

Correct Answer: C
Topic: Business Impact Analysis
Explanation: The Business Impact Analysis (BIA) should identify critical business processes first, as these processes determine recovery priorities and help guide the creation of recovery strategies.

QUESTION 1186
Which of the following activities should the business continuity manager perform FIRST after the replacement of hardware at the primary information processing facility?
- Verify compatibility with the hot site.
- Review the implementation report.
- Perform a walk-through of the disaster recovery plan.
- Update the IS assets inventory.

Correct Answer: D
Topic: Business Continuity Plan Implementation
Explanation: The IS asset inventory should be updated immediately after any hardware replacement to ensure the business continuity plan accurately reflects the organization's current infrastructure.

QUESTION 1187
Which of the following would contribute MOST to an effective business continuity plan (BCP)?
- Document is circulated to all interested parties
- Planning involves all user departments
- Approval by senior management
- Audit by an external IS auditor

Correct Answer: B
Topic: Effective Business Continuity Planning
Explanation: Involvement of user departments is crucial for identifying the critical business processes and priorities, which are central to a successful BCP.

QUESTION 1189
To develop a successful business continuity plan, end user involvement is critical during which of the following phases?
- Business recovery strategy
- Detailed plan development
- Business impact analysis (BIA)
- Testing and maintenance

Correct Answer: C
Topic: Business Continuity Planning Phases
Explanation: End user involvement during the BIA phase is vital for understanding the organization's operations and identifying the impact of potential disruptions on those operations.

QUESTION 1190
Which of the following would an IS auditor consider to be the MOST important to review when conducting a business continuity audit?
- A hot site is contracted for and available as needed.
- A business continuity manual is available and current.
- Insurance coverage is adequate and premiums are current.

- Media backups are performed on a timely basis and stored offsite.

Correct Answer: D
Topic: Business Continuity Audit Focus Areas
Explanation: Ensuring that media backups are performed regularly and stored offsite is essential for data recovery after a disaster. Without these backups, other recovery efforts would be ineffective.

QUESTION 1191
The PRIMARY objective of business continuity and disaster recovery plans should be to:
- Safeguard critical IS assets.
- Provide for continuity of operations.
- Minimize the loss to an organization.
- Protect human life.

Correct Answer: D
Topic: Business Continuity and Disaster Recovery Objectives
Explanation: The primary objective of any disaster recovery or business continuity plan is to protect human life, as it is the highest priority in any emergency situation.

QUESTION 1192
After a full operational contingency test, an IS auditor performs a review of the recovery steps. The auditor concludes that the time it took for the technological environment and systems to return to full-functioning exceeded the required critical recovery time. Which of the following should the auditor recommend?
- Perform an integral review of the recovery tasks.
- Broaden the processing capacity to gain recovery time.
- Make improvements in the facility's circulation structure.
- Increase the amount of human resources involved in the recovery.

Correct Answer: A
Topic: Recovery Time Improvement
Explanation: Performing an exhaustive review of the recovery tasks would be appropriate to identify where delays occurred and which tasks need to be adjusted to meet the recovery time objective.

QUESTION 1193
Which of the following is a continuity plan test that uses actual resources to simulate a system crash to cost-effectively obtain evidence about the plan's effectiveness?
- Paper test
- Post test
- Preparedness test
- Walkthrough

Correct Answer: C
Topic: Continuity Plan Testing
Explanation: A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness.

QUESTION 1194
While designing the business continuity plan (BCP) for an airline reservation system, the MOST appropriate method of data transfer/backup at an offsite location would be:
- Shadow file processing.
- Electronic vaulting.
- Hard-disk mirroring.
- Hot-site provisioning.

Correct Answer: A
Topic: Data Transfer and Backup Methods

Explanation: In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files, such as airline booking systems.

QUESTION 1195
Depending on the complexity of an organization's business continuity plan (BCP), the plan may be developed as a set of more than one plan to address various aspects of business continuity and disaster recovery, in such an environment, it is essential that:

- Each plan is consistent with one another.
- All plans are integrated into a single plan.
- Each plan is dependent on one another.
- The sequence for implementation of all plans is defined.

Correct Answer: A
Topic: Integration and Consistency in BCPs
Explanation: Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery. These do not necessarily have to be integrated into one single plan. However, each plan has to be consistent with others to have a viable business continuity.

QUESTION 1196
During a business continuity audit an IS auditor found that the business continuity plan (BCP) covered only critical processes. The IS auditor should:

- Recommend that the BCP cover all business processes.
- Assess the impact of the processes not covered.
- Report the findings to the IT manager.
- Redefine critical processes.

Correct Answer: B
Topic: Business Continuity Plan Scope
Explanation: The business impact analysis needs to be either updated or revisited to assess the risk of not covering all processes in the plan. It is possible that the cost of including all processes might exceed the value of those processes; therefore, they should not be covered.

QUESTION 1197
An IS auditor noted that an organization had adequate business continuity plans (BCPs) for each individual process, but no comprehensive BCP. Which would be the BEST course of action for the IS auditor?

- Recommend that an additional comprehensive BCP be developed.
- Determine whether the BCPs are consistent.
- Accept the BCPs as written.
- Recommend the creation of a single BCP.

Correct Answer: B
Topic: Business Continuity Planning Integration
Explanation: It is essential that the individual plans for each department or process are consistent with each other. There is no immediate need to combine them into one comprehensive plan unless inconsistencies or gaps are identified.

QUESTION 1198
When developing a business continuity plan (BCP), which of the following tools should be used to gain an understanding of the organization's business processes?

- Business continuity self-audit
- Resource recovery analysis
- Risk assessment
- Gap analysis

Correct Answer: C
Topic: Understanding Business Processes for BCP
Explanation: A risk assessment helps to identify potential threats and impacts to the organization, providing a basis for understanding business processes and their vulnerability in the event of a disaster.

QUESTION 1199
During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled FIRST?

- Evacuation plan
- Recovery priorities
- Backup storages
- Call tree

Correct Answer: A
Topic: Evacuation and Safety in BCPs
Explanation: The safety of human resources is the highest priority during any disaster. Reconciling evacuation plans ensures that there are no conflicts in how employees and other personnel will be evacuated from the building.

QUESTION 1200
Management considered two projections for its business continuity plan; plan A with two months to recover and plan B with eight months to recover. The recovery objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

- Downtime costs.
- Resumption costs.
- Recovery costs.
- Walkthrough costs.

Correct Answer: A
Topic: Business Continuity Plan Cost Evaluation
Explanation: Since the recovery time is longer in plan B, the downtime costs will likely be higher due to prolonged business disruptions.