QUESTION 1301
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
Correct Answer: B, C, D
Section: Mixed Questions
Explanation:
Biometric performance is evaluated based on metrics such as the false accept rate (FAR), false reject rate (FRR), and failure to enroll rate (FER), which assess errors in authentication and enrollment processes.

QUESTION 1302
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
Correct Answer: B
Section: Mixed Questions
Explanation:
The False Accept Rate (FAR) measures the percentage of invalid users who are mistakenly accepted by the biometric system, reflecting a critical performance metric in biometric security.

QUESTION 1303
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
Correct Answer: A, B
Section: Mixed Questions
Explanation:
An accurate biometric system typically exhibits low Equal Error Rate (EER) and low Crossover Error Rate (CER), both of which indicate that the system is effective at distinguishing between valid and invalid users without excessive errors.

QUESTION 1304
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

Correct Answer: E
Section: Mixed Questions
Explanation:
WEP (Wired Equivalent Privacy) uses the RC4 stream cipher for confidentiality and the CRC-32 checksum for integrity as part of the IEEE 802.11 standard.

QUESTION 1305
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
Correct Answer: A
Section: Mixed Questions
Explanation:
WEP uses the CRC-32 checksum for ensuring data integrity in addition to RC4 for confidentiality.

QUESTION 1306
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
Correct Answer: B
Section: Mixed Questions
Explanation:
WEP systems typically require keys in hexadecimal format, which can be easily guessed if they are based on simple patterns.

QUESTION 1307
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
Correct Answer: A
Section: Mixed Questions
Explanation:
Wi-Fi Protected Access (WPA/WPA2) implements most of the IEEE 802.11i standard, enhancing security over WEP with improvements like TKIP.

QUESTION 1308
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
Correct Answer: E
Section: Mixed Questions
Explanation:
WPA uses the Temporal Key Integrity Protocol (TKIP), which dynamically changes encryption keys to enhance security compared to WEP.

QUESTION 1309
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
Correct Answer: B
Section: Mixed Questions
Explanation:
A block cipher is a symmetric key cipher that processes fixed-length blocks of data with an unchanging transformation.

QUESTION 1310
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
Correct Answer: A
Section: Mixed Questions
Explanation:
A honeypot is a security resource designed to attract attackers, consisting of a computer or network site that appears legitimate but is isolated and prepared for detection.

QUESTION 1311
Which of the following is a tool you can use to simulate a big network structure on a single computer?
A) Honeymoon
B) Honeytrap
C) Honeytube
D) Honeyd
E) None of the choices
Correct Answer: D
Section: Mixed Questions
Explanation:
Honeyd is a software tool used to simulate a large network structure on a single computer, often for use with honeypots.

QUESTION 1312
Which of the following are valid choices for the Apache/SSL combination (choose all that apply):
A) The Apache-SSL project
B) Third-party SSL patches
C) The mod_ssl module
D) The mod_css module
E) None of the choices
Correct Answer: A, B, C
Section: Mixed Questions
Explanation:
Valid choices for the Apache/SSL combination include the Apache-SSL project, third-party SSL patches, and the mod_ssl module for securing Apache web servers.

QUESTION 1313
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
Correct Answer: A
Section: Mixed Questions
Explanation:
The primary purpose of a rootkit is to hide evidence of malicious activity from system administrators, making it difficult to detect unauthorized access or actions.

QUESTION 1314
Most Trojan horse programs are spread through:
A) E-mails
B) MP3
C) MS Office
D) Word template
E) None of the choices
Correct Answer: A
Section: Mixed Questions
Explanation:
Most Trojan horse programs are distributed via e-mails, often bundled with malicious attachments that execute harmful actions when opened.

QUESTION 1314
The Trojan.Linux.JBellz Trojan horse runs as a malformed file of what format?
A) E-mails
B) MP3
C) MS Office
D) Word template
E) None of the choices
Correct Answer: B
Section: Mixed Questions
Explanation:
The Trojan.Linux.JBellz Trojan horse is distributed as a malformed MP3 file, exploiting vulnerabilities in Linux systems.

QUESTION 1315
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
Correct Answer: B
Section: Mixed Questions
Explanation:
Keystroke logging, initially used as a diagnostic tool to measure productivity or errors, is now often used for malicious surveillance as spyware.

QUESTION 1316
You should know the difference between an exploit and a vulnerability. Which of the following refers to a weakness in the system?
A) Exploit
B) Vulnerability
C) Both
Correct Answer: B
Section: Mixed Questions
Explanation:
A vulnerability refers to a weakness in the system, while an exploit refers to a method or tool used to take advantage of that weakness.

QUESTION 1317
Which of the following is a rewrite of ipfwadm?
A) ipchains
B) iptables
C) Netfilter
D) ipcook
E) None of the choices
Correct Answer: A
Section: Mixed Questions
Explanation:
ipchains is a rewrite of the ipfwadm firewall, used in earlier versions of Linux, and it was later superseded by iptables.

QUESTION 1318
Iptables is based on which of the following frameworks?
- A) Netfilter
- B) NetDoom
- C) NetCheck
- D) NetSecure
- E) None of the choices

Correct Answer: A
Section: Mixed Questions
Explanation:
Iptables is based on the Netfilter framework, which provides hooks for intercepting and manipulating network packets in the Linux kernel. It controls packet filtering and NAT (Network Address Translation) within the Linux kernel.

QUESTION 1319
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

Correct Answer: B
Section: Mixed Questions
Explanation:
Cisco IOS-based routers use access control lists (ACLs) to filter traffic on the network edge. These lists can allow or deny traffic based on factors like IP addresses, protocols, and port numbers.

QUESTION 1320
Which of the following correctly describes 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

Correct Answer: B
Section: Mixed Questions
Explanation:
Wi-Fi Protected Access (WPA/WPA2) may cause compatibility issues, especially with older wireless access points that do not support the required WPA standards, even though WPA is designed to work with most wireless network interface cards.

QUESTION 1321
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

Correct Answer: A
Section: Mixed Questions
Explanation:
Federal Information Processing Standards (FIPS) are developed by the U.S. Federal government and are used by nonmilitary government agencies and government contractors. They ensure compliance with specific security and interoperability requirements.

QUESTION 1322
The Federal Information Processing Standards (FIPS) are primarily for use by (choose all that apply):
- A) All non-military government agencies
- B) US government contractors
- C) All military government agencies
- D) All private and public colleges in the US
- E) None of the choices

Correct Answer: A, B
Section: Mixed Questions

Explanation:
FIPS standards are specifically for use by nonmilitary government agencies and U.S. government contractors, ensuring security and compliance across federal systems.

QUESTION 1323
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

Correct Answer: A, B, C, D
Section: Mixed Questions
Explanation:
Database systems implement security measures such as access control, auditing, encryption, and integrity controls to protect sensitive data and ensure its confidentiality, accuracy, and availability.

QUESTION 1324
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

Correct Answer: A
Section: Mixed Questions
Explanation:
Vulnerability assessments are essential for evaluating database security. These assessments help identify misconfigurations and known vulnerabilities, improving the overall security posture of the database.

QUESTION 1325
Which of the following refers to any authentication protocol that requires two independent ways to establish identity and privileges?

- A) Strong-factor authentication
- B) Two-factor authentication
- C) Dual-password authentication
- D) Two-passphrases authentication
- E) Dual-keys authentication
- F) Rich-factor authentication

Correct Answer: B
Section: Mixed Questions
Explanation:
Two-factor authentication (TFA) involves using two independent factors to verify identity. Commonly, this involves 'something you know' (e.g., password) and 'something you have' (e.g., token), providing stronger security than single-factor authentication.

QUESTION 1326
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

Correct Answer: A, B, C
Section: Mixed Questions
Explanation:
Strong authentication typically requires two or more of the following: 'something you know' (password), 'something you have' (token), and 'something you are' (biometrics). This enhances security compared to single-factor authentication.

QUESTION 1327
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

Correct Answer: A, B, C, D
Section: Mixed Questions
Explanation:
Transactional controls are essential for improving efficiency. They reduce costs, shorten contract cycle times, improve procurement decisions, and help mitigate legal risks by monitoring and measuring contract performance.

QUESTION 1328
In the context of physical access control, what is known as the process of verifying user identities?

- A) Authentication
- B) Authorization
- C) Accounting
- D) Encryption
- E) Compression
- F) None of the choices

Correct Answer: A
Section: Mixed Questions
Explanation:
Authentication is the process of verifying the identity of a user, typically using one or more of the following factors: something you know, something you have, or something you are.

QUESTION 1329
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

Correct Answer: A, B
Section: Mixed Questions
Explanation:
Physical access control is enforced through means such as mechanical locks and guards. These methods restrict access to authorized personnel.

QUESTION 1330
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

Correct Answer: D
Section: Mixed Questions
Explanation:
Fault-tolerance is crucial in business-critical systems, where continuous operation is essential. It helps systems continue functioning despite hardware or software failures.

QUESTION 1331
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

Correct Answer: A
Section: Mixed Questions
Explanation:
Dumpster diving, or information diving, is the practice of sifting through commercial trash to gather sensitive or useful business information, such as passwords or confidential documents.

QUESTION 1332
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 the 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

Correct Answer: A
Section: Mixed Questions
Explanation:
A software audit is a key component of corporate risk management that helps organizations ensure they are using legally licensed software and avoid the risk of prosecution for software piracy.

QUESTION 1333
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

Correct Answer: A, B, C, D, E
Section: Mixed Questions
Explanation:
A mainframe audit ensures that processes are operating as required, that security measures are robust, that procedures are effective and updated, and that the system is secure and functioning as expected.

QUESTION 1334
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

Correct Answer: A, C
Section: Mixed Questions
Explanation:
A security server audit focuses on ensuring that segregation of duties is properly enforced, as well as maintaining a continuous and accurate audit trail to track system activity and potential security issues.

QUESTION 1335
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

Correct Answer: A, B, C, D, E
Section: Mixed Questions
Explanation:
An application system audit focuses on ensuring proper system performance, limiting unauthorized access, and verifying the accuracy of both input and output data, as well as ensuring that any system changes are properly authorized.

QUESTION 1336
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

Correct Answer: A
Section: Mixed Questions
Explanation:
An effective scoring system allows auditors to evaluate and prioritize risks, helping to establish a risk-based audit program. This system ensures that resources are focused on areas with the highest potential impact.

QUESTION 1337
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

Correct Answer: D
Section: Mixed Questions
Explanation:
The use of risk assessment tools should be formalized by developing written guidelines. These guidelines help auditors apply consistent and systematic approaches to classifying and managing risks.

QUESTION 1338
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

Correct Answer: B
Topic: Audit Methodology
Explanation:
To determine the appropriate level of audit coverage for the organization's IT environment, defining an effective assessment methodology is essential. This methodology allows for proper prioritization of audit resources and ensures the audit scope aligns with the organization's needs.

QUESTION 1339
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

Correct Answer: A
Topic: Risk-Based Auditing
Explanation:
IS audits should focus on areas with the highest risk and where there is the greatest opportunity for improvement. The purpose is to identify issues that can impact the organization’s efficiency, security, or performance.

QUESTION 1340
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

Correct Answer: A
Topic: Audit Reporting

Explanation:
The final audit report should only be issued once there is an agreement on the observations. This ensures that the audit findings are validated by the appropriate stakeholders.

QUESTION 1341
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

Correct Answer: A, B, C, D
Topic: Risk Assessment Guidelines
Explanation:
Well-written risk assessment guidelines should detail aspects like audit cycle lengths, timing of assessments, required documentation, and procedures for handling exceptions or special cases.

QUESTION 1342
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

Correct Answer: C
Topic: Audit Independence
Explanation:
The success of an internal IS audit depends largely on the independence of the audit team. Ensuring that the audit team is free from conflicts of interest or undue influence allows them to perform their work objectively and effectively.

QUESTION 1343
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

Correct Answer: A, B
Topic: Skills and Knowledge for IS Auditors
Explanation:
Personnel performing IS audits need to have adequate knowledge of the IT environment they are auditing and strong analytical skills to identify the underlying causes of any deficiencies or risks.

QUESTION 1344
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

Correct Answer: D
Topic: Audit Policy and Application Development
Explanation:
An IS audit policy should outline the role of internal auditors in key stages of application development, acquisition, and testing to ensure that security and controls are embedded throughout the process.

QUESTION 1345
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

Correct Answer: A
Topic: Auditing Application Acquisitions
Explanation:
For acquisitions with significant IT impacts, involving the IS audit team early in the due diligence stage helps identify potential risks and controls before proceeding with the acquisition.

QUESTION 1346
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

Correct Answer: D
Topic: Determining Audit Frequency
Explanation:
The frequency of IS audits should be based on the level and nature of risk present in the organization's systems. High-risk areas may require more frequent audits to ensure proper controls and security measures are in place.

QUESTION 1347
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

Correct Answer: A
Topic: Benefits of Risk-Based Audits
Explanation:
Risk-based audit programs enhance both the efficiency and effectiveness of audits by focusing on high-risk areas and ensuring resources are used appropriately to address the most critical issues.

QUESTION 1348
The sophistication and formality of IS audit programs may vary significantly depending on which of the following factors?

- A) The target's management hands-on involvement
- B) The target's location
- C) The target's size and complexity
- D) The target's budget
- E) The target's head count
- F) None of the choices

Correct Answer: C
Topic: Factors Affecting Audit Complexity
Explanation:
The complexity and scope of IS audit programs can vary based on the size and complexity of the organization being audited. Larger or more complex organizations require more detailed and formal audit processes.

QUESTION 1349
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

Correct Answer: A
Topic: Spyware Distribution Methods
Explanation:
Spyware is often distributed as a Trojan horse, where it is bundled with a seemingly harmless program that, once installed, secretly installs the spyware on the user's system.

QUESTION 1350
Which of the following is not a good tactic to use against hackers?

- A) Enticement
- B) Entrapment

Correct Answer: B
Topic: Countermeasures Against Hackers
Explanation:
Entrapment involves encouraging someone to commit a crime, which is illegal and unethical. It is not a good tactic for dealing with hackers. Enticement, on the other hand, is the practice of luring a hacker into a "honey pot," which can be used for gathering intelligence without directly encouraging illegal behavior.

QUESTION 1351
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

Correct Answer: D
Topic: Backdoors in Hacking
Explanation:

A backdoor is a method for a hacker to bypass normal authentication procedures and gain access to a system. It allows them to return to the system at will without being detected.

QUESTION 1352
A Trojan horse simply cannot operate autonomously.

- A) True
- B) False

Correct Answer: A
Topic: Trojan Horses
Explanation:
A Trojan horse requires the user to invoke the malicious code, meaning it cannot operate by itself without user interaction. It is disguised as a legitimate program or file.

QUESTION 1353
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

Correct Answer: C
Topic: Access Control
Explanation:
Logical access control refers to the policies and procedures designed to limit access to computer systems.