QUESTION 701
The reliability of an application system's audit trail may be questionable if:
- user IDs are recorded in the audit trail.
- the security administrator has read-only rights to the audit file.
- date and time stamps are recorded when an action occurs.
- users can amend audit trail records when correcting system errors.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
An audit trail is not effective if the details in it can be amended.

QUESTION 702
Which of the following user profiles should be of MOST concern to an IS auditor when performing an audit of an EFT system?
- Three users with the ability to capture and verify their own messages
- Five users with the ability to capture and send their own messages
- Five users with the ability to verify other users and to send their own messages
- Three users with the ability to capture and verify the messages of other users and to send their own messages

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The ability of one individual to capture and verify messages represents inadequate segregation since messages can be taken as correct and as if they had already been verified.

QUESTION 703
An IS auditor performing an independent classification of systems should consider a situation where functions could be performed manually at a tolerable cost for an extended period of time as:
- critical.
- vital.
- sensitive.
- noncritical.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Sensitive functions are best described as those that can be performed manually at a tolerable cost for an extended period of time. Critical functions are those that cannot be performed unless they are replaced by identical capabilities and cannot be replaced by manual methods. Vital functions refer to those that can be performed manually but only for a brief period of time; this is associated with lower costs of disruption than critical functions. Noncritical functions may be interrupted for an extended period at little or no cost to the company and require little time or cost to restore.

QUESTION 704
The implementation of access controls FIRST requires:
- a classification of IS resources.
- the labeling of IS resources.
- the creation of an access control list.
- an inventory of IS resources.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The implementation of access controls begins with an inventory of IS resources to understand what needs to be protected.

QUESTION 705
Which of the following is an example of the defense-in-depth security principle?
- Using two firewalls of different vendors to consecutively check the incoming network traffic
- Using a firewall as well as logical access controls on the hosts to control incoming network traffic
- Having no physical signs on the outside of a computer center building
- Using two firewalls in parallel to check different types of incoming traffic

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Defense in depth means using different security mechanisms that back each other up. When network traffic passes the firewall unintentionally, the logical access controls form a second line of defense. Using two firewalls of different vendors to consecutively check the incoming network traffic is an example of diversity in defense. The firewalls are the same security mechanisms. By using two different products, the probability of both products having the same vulnerabilities is diminished. Having no physical signs on the outside of a computer center building is a single security measure. Using two firewalls in parallel to check different types of incoming traffic is a single security mechanism and therefore no different than having a single firewall checking all traffic.

QUESTION 706
Which of the following would be the BEST access control procedure?
- The data owner formally authorizes access, and an administrator implements the user authorization tables.
- Authorized staff implements the user authorization tables and the data owner sanctions them.
- The data owner and an IS manager jointly create and update the user authorization tables.
- The data owner creates and updates the user authorization tables.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The data owner holds the privilege and responsibility for formally establishing the access rights. An IS administrator should then implement or update user authorization tables. Choice B alters the desirable order. Choice C is not a formal procedure for authorizing access.

QUESTION 707
Which of the following would MOST effectively reduce social engineering incidents?
- Security awareness training
- Increased physical security measures
- E-mail monitoring policy
- Intrusion detection systems

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Social engineering exploits human nature and weaknesses to obtain information and access privileges. By increasing employee awareness of security issues, it is possible to reduce the number of successful social engineering incidents. In most cases, social engineering incidents do not require the physical presence of the intruder. Therefore, increased physical security measures would not prevent the intrusion. An e-mail monitoring policy informs users that all e-mail in the organization is subject to monitoring; it does not protect the users from potential security incidents and intruders. Intrusion detection systems are used to detect irregular or abnormal traffic patterns.

QUESTION 708
An information security policy stating that "the display of passwords must be masked or suppressed" addresses which of the following attack methods?

- Piggybacking
- Dumpster diving
- Shoulder surfing
- Impersonation

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
If a password is displayed on a monitor, any person nearby could look over the shoulder of the user to obtain the password. Piggybacking refers to unauthorized persons following, either physically or virtually, authorized persons into restricted areas. Masking the display of passwords would not prevent someone from tailgating an authorized person. This policy only refers to "the display of passwords." If the policy referred to "the display and printing of passwords," then it would address shoulder surfing and dumpster diving (looking through an organization's trash for valuable information). Impersonation refers to someone acting as an employee in an attempt to retrieve desired information.

QUESTION 709
To ensure compliance with a security policy requiring that passwords be a combination of letters and numbers, an IS auditor should recommend that:

- the company policy be changed.
- passwords are periodically changed.
- an automated password management tool be used.
- security awareness training is delivered.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The use of an automated password management tool is a preventive control measure. The software would prevent repetition (semantic) and enforce syntactic rules, thus making the passwords robust. It would also provide a method for ensuring frequent changes and would prevent the same user from reusing their old password for a designated period. Choices A, B, and D do not enforce compliance.

QUESTION 710
An IS auditor has identified the lack of an authorization process for users of an application. The IS auditor's main concern should be that:

- more than one individual can claim to be a specific user.
- there is no way to limit the functions assigned to users.
- user accounts can be shared.
- users have a need-to-know privilege.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Without an appropriate authorization process, it will be impossible to establish functional limits and accountability. The risk that more than one individual can claim to be a specific user is associated with the authentication processes, rather than with authorization. The risk that user accounts can be shared is associated with identification processes, rather than with authorization. The need-to-know basis is the best approach to assigning privileges during the authorization process.

QUESTION 711
An IS auditor reviewing digital rights management (DRM) applications should expect to find an extensive use for which of the following technologies?

- Digitalized signatures
- Hashing
- Parsing
- Steganography

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Steganography is a technique for concealing the existence of messages or information. An increasingly important steganographical technique is digital watermarking, which hides data within data, e.g., by encoding rights information in a picture or music file without altering the picture or music's perceivable aesthetic qualities. Digitalized signatures are not related to digital rights management. Hashing creates a message hash or digest, which is used to ensure the integrity of the message; it is usually considered a part of cryptography. Parsing is the process of splitting up a continuous stream of characters for analytical purposes and is widely applied in the design of programming languages or in data entry editing.

QUESTION 712
The information security policy that states "each individual must have their badge read at every controlled door" addresses which of the following attack methods?

- Piggybacking
- Shoulder surfing
- Dumpster diving
- Impersonation

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Piggybacking refers to unauthorized persons following authorized persons, either physically or virtually, into restricted areas. This policy addresses the polite behavior problem of holding doors open for a stranger; if every employee must have their badge read at every controlled door, no unauthorized person could enter the sensitive area. Looking over the shoulder of a user to obtain sensitive information could be done by an unauthorized person who has gained access to areas using piggybacking, but this policy specifically refers to physical access control. Shoulder surfing would not be prevented by the implementation of this policy. Dumpster diving, looking through an organization's trash for valuable information, could be done outside the company's physical perimeter; therefore, this policy would not address this attack method. Impersonation refers to a social engineer acting as an employee trying to retrieve the desired information. Some forms of social engineering attacks could join an impersonation attack and piggybacking, but this information security policy does not address the impersonation attack.

QUESTION 713
Which of the following presents an inherent risk with no distinct identifiable preventive controls?

- Piggybacking
- Viruses
- Data diddling
- Unauthorized application shutdown

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Data diddling involves changing data before they are entered into the computer. It is one of the most common abuses because it requires limited technical knowledge and occurs before computer security can protect the data. There are only compensating controls for data diddling. Piggybacking is the act of following an authorized person through a secured door and can be prevented by the use of deadman doors. Logical piggybacking is an attempt to gain access through someone who has the rights, e.g., electronically attaching to an authorized telecommunication link to possibly intercept transmissions. This could be prevented by encrypting the message. Viruses are malicious program code inserted into another executable code that can self-replicate and spread from computer to computer via sharing of computer diskettes, transfer of logic over telecommunication lines, or direct contact with an infected machine. Antiviral software can be used to protect the computer against viruses. The shutdown of an application

can be initiated through terminals or microcomputers connected directly (online) or indirectly (dial-up line) to the computer. Only individuals knowing the high-level logon ID and password can initiate the shutdown process, which is effective if there are proper access controls.

QUESTION 714
Which of the following is a general operating system access control function?
- Creating database profiles
- Verifying user authorization at a field level
- Creating individual accountability
- Logging database access activities for monitoring access violations

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Creating individual accountability is the function of the general operating system. Creating database profiles, verifying user authorization at a field level, and logging database access activities for monitoring access violations are all database-level access control functions.

QUESTION 715
Which of the following BEST restricts users to those functions needed to perform their duties?
- Application level access control
- Data encryption
- Disabling floppy disk drives
- Network monitoring device

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The use of application-level access control programs is a management control that restricts access by limiting users to only those functions needed to perform their duties. Data encryption and disabling floppy disk drives can restrict users to specific functions, but are not the best choices. A network monitoring device is a detective control, not a preventive control.

QUESTION 716
For a discretionary access control to be effective, it must:
- operate within the context of mandatory access controls.
- operate independently of mandatory access controls.
- enable users to override mandatory access controls when necessary.
- be specifically permitted by the security policy.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Discretionary access control (DAC) operates within the framework established by mandatory access controls (MAC). While DAC allows users some flexibility in controlling access, it still functions under the prohibition principle of MAC, where anything not expressly permitted is forbidden.

QUESTION 717
An IS auditor examining a biometric user authentication system establishes the existence of a control weakness that would allow an unauthorized individual to update the centralized database on the server that is used to store biometric templates. Of the following, which is the BEST control against this risk?
- Kerberos
- Vitality detection
- Multimodal biometrics
- Before-image/after-image logging

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Kerberos is a network authentication protocol that provides secure authentication, thereby preventing unauthorized access to the database. Vitality detection and multimodal biometrics primarily defend against spoofing, while before-image/after-image logging is a detective control, not preventative.

QUESTION 718
From a control perspective, the PRIMARY objective of classifying information assets is to:
- establish guidelines for the level of access controls that should be assigned.
- ensure access controls are assigned to all information assets.
- assist management and auditors in risk assessment.
- identify which assets need to be insured against losses.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Classifying information assets helps establish guidelines for access controls based on sensitivity and criticality. While it assists in risk assessment, the primary objective is to provide a framework for access control.

QUESTION 719
An organization has been recently downsized. In light of this, an IS auditor decides to test logical access controls. The IS auditor's PRIMARY concern should be that:
- all system access is authorized and appropriate for an individual's role and responsibilities.
- management has authorized appropriate access for all newly-hired individuals.
- only the system administrator has authority to grant or modify access to individuals.
- access authorization forms are used to grant or modify access to individuals.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Given the rapid personnel changes during downsizing, the auditor must ensure that access rights are still appropriate for each individual's new role and responsibilities and that access is revoked for those no longer with the organization.

QUESTION 720
The logical exposure associated with the use of a checkpoint restart procedure is:
- denial of service.
- an asynchronous attack.
- wire tapping.
- computer shutdown.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Checkpoint restart procedures can be susceptible to asynchronous attacks, where an attacker may manipulate parameters saved at checkpoints, potentially gaining higher access levels upon restart.

QUESTION 721
Inadequate programming and coding practices introduce the risk of:
- phishing.
- buffer overflow exploitation.
- SYN flood.
- brute force attacks.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Buffer overflow vulnerabilities arise from poor coding practices, allowing attackers to exploit these weaknesses. Phishing, SYN floods, and brute force attacks are not directly related to programming practices.

QUESTION 722
Which of the following would prevent unauthorized changes to information stored in a server's log?
- Write-protecting the directory containing the system log.
- Writing a duplicate log to another server.
- Daily printing of the system log.
- Storing the system log in write-once media.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Using write-once media ensures the log cannot be altered once written. Write protection can be bypassed by privileged users, and duplicate logs or printed logs do not prevent modifications to the original.

QUESTION 723
After reviewing its business processes, a large organization is deploying a new web application based on VoIP technology. Which of the following is the MOST appropriate approach for implementing access control that will facilitate security management of the VoIP web application?
- Fine-grained access control
- Role-based access control (RBAC)
- Access control lists
- Network/service access control

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
RBAC is suitable for large systems, enabling effective management of user access based on roles. Fine-grained access and access control lists may not scale efficiently for enterprise-wide systems.

QUESTION 724
In an online banking application, which of the following would BEST protect against identity theft?
- Encryption of personal password
- Restricting the user to a specific terminal
- Two-factor authentication
- Periodic review of access logs

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Two-factor authentication enhances security by requiring two forms of identification, making it significantly harder for unauthorized individuals to impersonate legitimate users.

QUESTION 725
Which of the following is the BEST method for preventing the leakage of confidential information in a laptop computer?
- Encrypt the hard disk with the owner's public key.
- Enable the boot password (hardware-based password).
- Use a biometric authentication device.
- Use two-factor authentication to log on to the notebook.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Encrypting the hard disk with a strong key ensures that confidential information remains secure, even if the device is lost. Authentication methods do not prevent data leakage if the device is physically compromised.

QUESTION 726
The responsibility for authorizing access to application data should be with the:
- data custodian.
- database administrator (DBA).
- data owner.
- security administrator.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Data owners are responsible for granting access to their data. DBAs manage databases, and security administrators implement security policies, but data ownership confers the authority for access.

QUESTION 727
During an audit of the logical access control of an ERP financial system, an IS auditor found some user accounts shared by multiple individuals. The user IDs were based on roles rather than individual identities. What should the IS auditor do next?
- Look for compensating controls.
- Review financial transactions logs.
- Review the scope of the audit.
- Ask the administrator to disable these accounts.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The auditor should evaluate the effectiveness of compensating controls since the best practice is to have unique user IDs for accountability. Other actions might disrupt necessary access without understanding the context.

QUESTION 728
Minimum password length and password complexity verification are examples of:
- detection controls.
- control objectives.
- audit objectives.
- control procedures.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
These are control procedures established to ensure users create strong passwords, thus serving as preventive measures against unauthorized access.

QUESTION 729
An IS auditor finds that a DBA has read and write access to production data. The IS auditor should:
- accept the DBA access as a common practice.
- assess the controls relevant to the DBA function.
- recommend the immediate revocation of the DBA access to production data.
- review user access authorizations approved by the DBA.

Correct Answer: B

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Evaluating the controls surrounding DBA access is crucial, as such access can be necessary for legitimate tasks. Revocation should not be immediate without understanding the access's context.

QUESTION 730
When using a universal storage bus (USB) flash drive to transport confidential corporate data to an offsite location, an effective control would be to:

- carry the flash drive in a portable safe.
- assure management that you will not lose the flash drive.
- request that management deliver the flash drive by courier.
- encrypt the folder containing the data with a strong key.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Encrypting the data on the flash drive ensures its security, regardless of physical loss. Other methods do not adequately protect against data breaches if the device is lost or stolen.

QUESTION 731
A business application system accesses a corporate database using a single ID and password embedded in a program. Which would provide efficient access control?

- Apply role-based permissions within the application system.
- Introduce a secondary authentication method such as card swipe.
- Have users input the ID and password for each database transaction.
- Set an expiration period for the database password embedded in the program.

Correct Answer: Apply role-based permissions within the application system.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Role-based access control effectively manages permissions by assigning roles to users, addressing the main issue of user permissions.

QUESTION 732
Which is the BEST practice to ensure that access authorizations are still valid?

- Information owner provides authorization for users to gain access.
- Identity management is integrated with human resource processes.
- Information owners periodically review the access controls.
- An authorization matrix is used to establish validity of access.

Correct Answer: Identity management is integrated with human resource processes.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: This integration ensures timely adjustments to access rights when personnel changes occur, reducing risks from authorization creep.

QUESTION 733
What would be of GREATEST concern during a forensic investigation after a technical lead leaves the organization?

- Audit logs are not enabled for the system.
- A logon ID for the technical lead still exists.
- Spyware is installed on the system.
- A Trojan is installed on the system.

Correct Answer: Audit logs are not enabled for the system.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Without audit logs, misuse of the logon ID is difficult to prove, hindering investigation efforts.

QUESTION 734
What would be an effective access control for an ERP application?
- User-level permissions.
- Role-based.
- Fine-grained.
- Discretionary.

Correct Answer: Role-based.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Role-based access control simplifies management by grouping users, while user-level permissions create overhead.

QUESTION 735
What should be the GREATEST concern regarding portable media used by employees?
- The copying of sensitive data on them.
- The copying of songs and videos on them.
- The cost of these devices multiplied by all the employees could be high.
- They facilitate the spread of malicious code through the corporate network.

Correct Answer: The copying of sensitive data on them.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data leakage is a significant risk, especially sensitive information, if devices are lost or stolen.

QUESTION 736
Who should authorize access rights to production data and systems?
- Process owners.
- System administrators.
- Security administrator.
- Data owners.

Correct Answer: Data owners.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data owners are responsible for safeguarding and granting access to production data on a need-to-know basis.

QUESTION 737
An IS auditor has completed a network audit. Which of the following is the MOST significant logical security finding?
- Network workstations are not disabled automatically after a period of inactivity.
- Wiring closets are left unlocked.
- Network operating manuals and documentation are not properly secured.
- Network components are not equipped with an uninterruptible power supply.

Correct Answer: Network workstations are not disabled automatically after a period of inactivity.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Disabling inactive workstations restricts unauthorized access, making it a critical finding in logical security.

QUESTION 738
Which of the following would MOST effectively enhance the security of a challenge-response-based authentication system?
- Selecting a more robust algorithm to generate challenge strings.
- Implementing measures to prevent session hijacking attacks.
- Increasing the frequency of associated password changes.
- Increasing the length of authentication strings.

Correct Answer: Implementing measures to prevent session hijacking attacks.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Addressing the risk of session hijacking is critical for the effectiveness of challenge-response authentication.

QUESTION 739
Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in the data warehouse?

- Implement column- and row-level permissions.
- Enhance user authentication via strong passwords.
- Organize the data warehouse into subject matter-specific databases.
- Log user access to the data warehouse.

Correct Answer: Implement column- and row-level permissions.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Column- and row-level security can prevent unauthorized access to sensitive data, providing a fine-grained security model.

QUESTION 740
The responsibility for authorizing access to a business application system belongs to the:

- Data owner.
- Security administrator.
- IT security manager.
- Requestor's immediate supervisor.

Correct Answer: Data owner.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Data owners are responsible for authorizing access to applications and backend databases.

QUESTION 741
An organization has created a policy that defines the types of websites that users are forbidden to access. What is the MOST effective technology to enforce this policy?

- Stateful inspection firewall.
- Web content filter.
- Web cache server.
- Proxy server.

Correct Answer: Web content filter.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A web content filter can accept or deny web communications based on configured rules, effectively enforcing access policies.

QUESTION 742
What would be the MOST effective control for enforcing accountability among database users accessing sensitive information?

- Implement a log management process.
- Implement a two-factor authentication.
- Use table views to access sensitive data.
- Separate database and application servers.

Correct Answer: Implement a log management process.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A log management process creates and stores logs with pertinent information, enforcing accountability by tracking user actions.

QUESTION 743

Which of the following intrusion detection systems (IDSs) monitors the general patterns of activity and traffic on a network and creates a database?

- Signature-based.
- Neural networks-based.
- Statistical-based.
- Host-based.

Correct Answer: Neural networks-based.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Neural networks-based IDSs monitor general patterns of activity, similar to statistical models but with self-learning capabilities.

QUESTION 744
The MOST important difference between hashing and encryption is that hashing:

- Is irreversible.
- Output is the same length as the original message.
- Is concerned with integrity and security.
- Is the same at the sending and receiving end.

Correct Answer: Is irreversible.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Hashing creates a one-way output that cannot be reversed, unlike encryption, which is reversible.

QUESTION 745
Which of the following cryptography options would increase overhead/cost?

- The encryption is symmetric rather than asymmetric.
- A long asymmetric encryption key is used.
- The hash is encrypted rather than the message.
- A secret key is used.

Correct Answer: A long asymmetric encryption key is used.
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Longer asymmetric encryption keys require significantly more processing time, increasing overhead.

QUESTION 746
The MOST important success factor in planning a penetration test is:

- The documentation of the planned testing procedure.
- Scheduling and deciding on the timed length of the test.
- The involvement of the management of the client organization.
- The qualifications and experience of staff involved in the test.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The most important part of planning any penetration test is the involvement of the management of the client organization. Penetration testing without management approval could reasonably be considered espionage and is illegal in many jurisdictions.

QUESTION 747
Which of the following virus prevention techniques can be implemented through hardware?

- Remote booting
- Heuristic scanners
- Behavior blockers

- Immunizers

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Remote booting (e.g., diskless workstations) is a method of preventing viruses and can be implemented through hardware. Behavior blockers are detection-based rather than prevention-based, and choices B and D are not hardware-based.

QUESTION 748
Which of the following append themselves to files as a protection against viruses?

- Behavior blockers
- Cyclical redundancy checkers (CRCs)
- Immunizers
- Active monitors

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Immunizers defend against viruses by appending sections of themselves to files. They continuously check the file for changes and report changes as possible viral behavior.

QUESTION 749
Which of the following acts as a decoy to detect active internet attacks?

- Honeypots
- Firewalls
- Trapdoors
- Traffic analysis

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Honeypots are computer systems set up to attract and trap individuals attempting to penetrate systems. They help gather data on attack methods to improve future security measures.

QUESTION 750
A certificate authority (CA) can delegate the processes of:

- Revocation and suspension of a subscriber's certificate.
- Generation and distribution of the CA public key.
- Establishing a link between the requesting entity and its public key.
- Issuing and distributing subscriber certificates.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Establishing a link between the requesting entity and its public key is typically a function of a registration authority, which can be delegated by the CA. Other functions, like revocation and key management, are handled directly by the CA.

QUESTION 751
Which of the following results in a denial-of-service attack?

- Brute force attack
- Ping of death
- Leapfrog attack
- Negative acknowledgement (NAK) attack

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation: A Ping of Death attack sends a packet larger than 65 KB without a fragmentation flag, causing a denial of service. Brute force, leapfrog, and NAK attacks have different purposes.

QUESTION 752

Which of the following is the GREATEST advantage of elliptic curve encryption over RSA encryption?

- Computation speed
- Ability to support digital signatures
- Simpler key distribution
- Greater strength for a given key length

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The main advantage of elliptic curve encryption over RSA is its faster computation speed, while providing the same level of security with shorter key lengths.

QUESTION 753
Which of the following would be the BEST overall control for an Internet business looking for confidentiality, reliability, and integrity of data?

- Secure Sockets Layer (SSL)
- Intrusion detection system (IDS)
- Public key infrastructure (PKI)
- Virtual private network (VPN)

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: PKI is the best overall solution for ensuring confidentiality, reliability, and integrity, as it supports encryption, digital signatures, and non-repudiation.

QUESTION 754
To ensure message integrity, confidentiality, and non-repudiation between two parties, the MOST effective method would be to create a message digest by applying a cryptographic hashing algorithm against:

- The entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering the key by using the receiver's public key.
- Any part of the message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering the key using the receiver's public key.
- The entire message, enciphering the message digest using the sender's private key, enciphering the message with a symmetric key, and enciphering both the encrypted message and digest using the receiver's public key.
- The entire message, enciphering the message digest using the sender's private key and enciphering the message using the receiver's public key.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: This method ensures message integrity by applying a cryptographic hashing algorithm to the entire message and confidentiality through symmetric key encryption, with the symmetric key being encrypted by the receiver’s public key.

QUESTION 755
Which of the following antivirus software implementation strategies would be the MOST effective in an interconnected corporate network?

- Server antivirus software
- Virus walls
- Workstation antivirus software
- Virus signature updating

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Virus walls, integrated with firewalls, detect and remove viruses before they enter the network, providing effective early-stage protection.

QUESTION 756
Which of the following would be of MOST concern to an IS auditor reviewing a virtual private network (VPN) implementation? Computers on the network that are located:
- On the enterprise's internal network.
- At the backup site.
- In employees' homes.
- At the enterprise's remote offices.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Home computers pose the greatest risk, as they are typically subject to less stringent security policies than corporate-managed systems, increasing the likelihood of introducing vulnerabilities to the VPN.

QUESTION 757
The PRIMARY reason for using digital signatures is to ensure data:
- Confidentiality.
- Integrity.
- Availability.
- Timeliness.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Digital signatures provide data integrity by ensuring that a document has not been altered after it was signed.

QUESTION 758
Which of the following is an example of a passive attack initiated through the Internet?
- Traffic analysis
- Masquerading
- Denial of service
- E-mail spoofing

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Passive attacks include activities like traffic analysis and eavesdropping, where the attacker monitors communication without altering it.

QUESTION 759
Transmitting redundant information with each character or frame to facilitate detection and correction of errors is called:
- Feedback error control.
- Block sum check.
- Forward error control.
- Cyclic redundancy check.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation: Forward error control transmits extra information with each frame, allowing the receiver to detect and correct errors, making it an efficient method of error control.

QUESTION 760
The security level of a private key system depends on the number of:
- Encryption key bits.
- Messages sent.
- Keys.

- Channels used.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation: The security level of a private key system is directly related to the number of encryption key bits used. The more bits in the key, the harder it is to break the encryption.

QUESTION 761
During what process should router access control lists be reviewed?

- **Environmental review**
- **Network security review**
- **Business continuity review**
- **Data integrity review**

Correct Answer: B
Explanation: Router access control lists should be reviewed during **network security reviews**. This process includes reviewing various network controls such as router access control lists, port scanning, and connections to both internal and external systems. Environmental, business continuity, and data integrity reviews typically do not involve checking router access control lists.

QUESTION 762
Which of the following components is responsible for the collection of data in an intrusion detection system (IDS)?

- **Analyzer**
- **Administration console**
- **User interface**
- **Sensor**

Correct Answer: D
Explanation: In an IDS, **sensors** are responsible for collecting data. **Analyzers** process the collected data to detect possible intrusions. The **administration console** and **user interface** are for managing and interacting with the system but are not directly involved in data collection.

QUESTION 763
Which of the following concerns associated with the World Wide Web would be addressed by a firewall?

- **Unauthorized access from outside the organization**
- **Unauthorized access from within the organization**
- **A delay in Internet connectivity**
- **A delay in downloading using File Transfer Protocol (FTP)**

Correct Answer: A
Explanation: Firewalls are designed to prevent unauthorized access from outside an organization. They act as barriers, blocking unapproved inbound traffic from the internet. They are not intended to address internal access issues or performance-related problems like delays in connectivity or FTP downloads.

QUESTION 764
A digital signature contains a message digest to:

- **Show if the message has been altered after transmission.**
- **Define the encryption algorithm.**
- **Confirm the identity of the originator.**
- **Enable message transmission in a digital format.**

Correct Answer: A
Explanation: The **message digest** included in a digital signature helps ensure data integrity by verifying if the message has been altered. The digest does not define the encryption algorithm or confirm the sender's identity but ensures that the content remains unchanged during transmission.

QUESTION 765
Which of the following manages the digital certificate life cycle to ensure adequate security and controls exist in digital signature applications related to e-commerce?

- **Registration authority**
- **Certificate authority (CA)**
- **Certification relocation list**
- **Certification practice statement**

Correct Answer: B
Explanation: A **Certificate Authority (CA)** is responsible for managing the lifecycle of digital certificates, including issuance, renewal, and revocation. It also maintains certificate directories and manages the Certificate Revocation List (CRL). A **registration authority** handles administrative tasks like certificate requests but does not manage the certificate lifecycle.

QUESTION 766
A TCP/IP-based environment is exposed to the Internet. Which of the following BEST ensures that complete encryption and authentication protocols exist for protecting information while transmitted?

- **Work is completed in tunnel mode with IP security using the nested services of authentication header (AH) and encapsulating security payload (ESP).**
- **A digital signature with RSA has been implemented.**
- **Digital certificates with RSA are being used.**
- **Work is being completed in TCP services.**

Correct Answer: A
Explanation: Using **tunnel mode with IP security (IPSec)** and employing the **Authentication Header (AH)** and **Encapsulating Security Payload (ESP)** services provides complete encryption and authentication for protecting information. The other options provide either authentication or encryption but not both.

QUESTION 767
Digital signatures require the:

- **Signer to have a public key and the receiver to have a private key.**
- **Signer to have a private key and the receiver to have a public key.**
- **Signer and receiver to have a public key.**
- **Signer and receiver to have a private key.**

Correct Answer: B
Explanation: In digital signature cryptography, the **signer uses a private key** to create the signature, and the **receiver uses the signer's public key** to verify the signature. This ensures that only the signer could have created the signature, and the recipient can confirm its authenticity.

QUESTION 768
The feature of a digital signature that ensures the sender cannot later deny generating and sending the message is called:

- **Data integrity.**
- **Authentication.**
- **Non-repudiation.**
- **Replay protection.**

Correct Answer: C
Explanation: Non-repudiation ensures that the sender cannot deny having generated and sent the message. It confirms the sender's identity and prevents them from claiming otherwise, which is a key feature of digital signatures.

QUESTION 769
An IS auditor doing penetration testing during an audit of internet connections would:

- **Evaluate configurations.**
- **Examine security settings.**
- **Ensure virus-scanning software is in use.**
- **Use tools and techniques available to a hacker.**

Correct Answer: D
Explanation: Penetration testing involves simulating hacker-like attacks on a system using the same tools and techniques a hacker might use. The other options are activities of an IS auditor but are not specific to penetration testing.

QUESTION 770
Which of the following should concern an IS auditor when reviewing security in a client-server environment?

- **Protecting data using an encryption technique**
- **Preventing unauthorized access using a diskless workstation**
- **The ability of users to access and modify the database directly**
- **Disabling floppy drives on the users' machines**

Correct Answer: C
Explanation: An IS auditor should be most concerned about users directly accessing and modifying a database because this could lead to data integrity issues. Other concerns, such as encryption and preventing copying, are secondary to this fundamental security concern.

QUESTION 771
Which of the following is a technique that could be used to capture network user passwords?

- **Encryption**
- **Sniffing**
- **Spoofing**
- **Data destruction**

Correct Answer: B
Explanation: Sniffing is a technique used to capture data packets traversing a network, which can include sensitive information like passwords. **Encryption** prevents unauthorized access to data, **spoofing** involves impersonating another entity, and **data destruction** involves deleting information.

QUESTION 772
Which of the following controls would BEST detect intrusion?

- **User IDs and user privileges are granted through authorized procedures.**
- **Automatic logoff is used when a workstation is inactive for a particular period of time.**
- **Automatic logoff of the system occurs after a specified number of unsuccessful attempts.**
- **Unsuccessful logon attempts are monitored by the security administrator.**

Correct Answer: D
Explanation: Monitoring **unsuccessful logon attempts** helps detect potential intrusions by tracking repeated failed attempts to access a system. The other options are preventative or reactive controls, but do not directly detect intrusion.

QUESTION 773
Which of the following is a feature of an intrusion detection system (IDS)?

- **Gathering evidence on attack attempts**
- **Identifying weaknesses in the policy definition**
- **Blocking access to particular sites on the Internet**
- **Preventing certain users from accessing specific servers**

Correct Answer: A
Explanation: An **IDS** gathers evidence on attack attempts or penetration efforts to identify possible intrusions. **Blocking access** and **preventing user access** are typically functions of a firewall, not an IDS.

QUESTION 774
An IS auditor performing a telecommunication access control review should be concerned PRIMARILY with the:

- **Maintenance of access logs of usage of various system resources.**
- **Authorization and authentication of the user prior to granting access to system resources.**
- **Adequate protection of stored data on servers by encryption or other means.**
- **Accountability system and the ability to identify any terminal accessing system resources.**

Correct Answer: B
Explanation: The primary concern in a **telecommunication access control review** is ensuring **authorization and authentication** are in place before granting access. This is a critical preventive control. Other choices are important but secondary concerns in this context.

QUESTION 775
Which of the following is the MOST effective type of antivirus software?

- **Scanners**
- **Active monitors**
- **Integrity checkers**
- **Vaccines**

Correct Answer: C
Explanation: Integrity checkers are highly effective as they verify the integrity of files by comparing them against a known baseline (often using a CRC or hash function). They can detect changes indicative of virus infections. **Scanners** and **vaccines** require regular updates to remain effective, while **active monitors** can sometimes cause false positives.

QUESTION 776
When using public key encryption to secure data being transmitted across a network:

- **Both the key used to encrypt and decrypt the data are public.**
- **The key used to encrypt is private, but the key used to decrypt the data is public.**
- **The key used to encrypt is public, but the key used to decrypt the data is private.**
- **Both the key used to encrypt and decrypt the data are private.**

Correct Answer: C
Explanation: In **public key encryption** (asymmetric encryption), the **public key** is used to encrypt the data, and the corresponding **private key** is used to decrypt it.

QUESTION 777
The technique used to ensure security in virtual private networks (VPNs) is:

- **Encapsulation**
- **Wrapping**
- **Transform**
- **Encryption**

Correct Answer: A
Explanation: Encapsulation, also known as **tunneling**, is a technique used in VPNs to securely transport data over networks by encapsulating it in another protocol. **Encryption** also plays a role, but encapsulation is the key technique in VPN security.

QUESTION 778
During an audit of a telecommunications system, an IS auditor finds that the risk of intercepting data transmitted to and from remote sites is very high. The MOST effective control for reducing this exposure is:

- **Encryption**
- **Callback modems**
- **Message authentication**
- **Dedicated leased lines**

Correct Answer: A
Explanation: Encryption is the most effective method to protect data in transit from being intercepted. **Callback modems** and **leased lines** offer some security but do not protect the data itself from being intercepted.

QUESTION 779
An internet-based attack using password sniffing can:

- **Enable one party to act as if they are another party.**
- **Cause modification to the contents of certain transactions.**
- **Be used to gain access to systems containing proprietary information.**
- **Result in major problems with billing systems and transaction processing agreements.**

Correct Answer: C
Explanation: Password sniffing allows attackers to gain access to systems containing sensitive information, such as proprietary data. The other options describe different types of attacks, such as **spoofing** and **data modification**.

QUESTION 780
Which of the following controls would be the MOST comprehensive in a remote access network with multiple and diverse subsystems?

- **Proxy server**
- **Firewall installation**
- **Network administrator**
- **Password implementation and administration**

Correct Answer: D
Explanation: Password implementation and administration is the most comprehensive control for a remote access network, as it ensures that only authorized users can access various subsystems. **Firewalls** and **proxy servers** are essential but are more specific controls.

QUESTION 781
An IS auditor notes that an organization's development team has too much access to the production environment. The PRIMARY concern is that this could:

- A. cause unintentional changes to the production environment.
- B. lead to unauthorized changes to business data.
- C. result in segregation of duties (SoD) conflicts.
- D. affect the quality assurance (QA) process.

Correct Answer: C
Explanation: The primary concern when a development team has too much access to the production environment is a segregation of duties (SoD) conflict. Developers with production access could make changes without appropriate approval or testing, leading to unauthorized changes or potentially harmful modifications in a live environment. While the other issues (like unintentional changes, changes to business data, and QA process impacts) are valid concerns, SoD conflicts are the most critical because they compromise internal controls designed to prevent fraud or errors.

QUESTION 782
When planning an audit of a network setup, an IS auditor should give highest priority to obtaining which of the following network documentation?

- A) **Wiring and schematic diagram**
- B) Users' lists and responsibilities
- C) Application lists and their details
- D) Backup and recovery procedures

Correct Answer: A
Explanation: The wiring and schematic diagram of the network is essential for carrying out a network audit. Without it, an audit may not be feasible. While the other documents are important, they are not as critical as understanding the physical and logical network layout.

QUESTION 783
Which of the following encrypt/decrypt steps provides the GREATEST assurance of achieving confidentiality, message integrity, and nonrepudiation by either sender or recipient?

- A) The recipient uses their private key to decrypt the secret key.
- B) The encrypted prehash code and the message are encrypted using a secret key.
- C) The encrypted prehash code is derived mathematically from the message to be sent.
- D) **The recipient uses the sender's public key, verified with a certificate authority, to decrypt the prehash code.**

Correct Answer: D
Explanation: The recipient can use the sender's public key to decrypt the prehash code, ensuring the message is authentic and unchanged, which provides assurance of confidentiality, message integrity, and nonrepudiation.

QUESTION 784
Use of asymmetric encryption in an internet e-commerce site, where there is one private key for the hosting server and the public key is widely distributed to the customers, is MOST likely to provide comfort to the:

- A) **Customer over the authenticity of the hosting organization.**
- B) Hosting organization over the authenticity of the customer.
- C) Customer over the confidentiality of messages from the hosting organization.
- D) Hosting organization over the confidentiality of messages passed to the customer.

Correct Answer: A
Explanation: The customer can be assured of the authenticity of the hosting organization because only the real site can encrypt with the private key, which the customer can decrypt with the public key.

QUESTION 785
E-mail message authenticity and confidentiality is BEST achieved by signing the message using the:

- A) **Sender's private key and encrypting the message using the receiver's public key.**
- B) Sender's public key and encrypting the message using the receiver's private key.
- C) Receiver's private key and encrypting the message using the sender's public key.
- D) Receiver's public key and encrypting the message using the sender's private key.

Correct Answer: A
Explanation: By signing with the sender's private key, the receiver can verify authenticity with the sender's public key. By encrypting the message with the receiver's public key, only the receiver can decrypt it.

QUESTION 786
An organization is considering connecting a critical PC-based system to the internet. Which of the following would provide the BEST protection against hacking?

- A) **An application-level gateway**
- B) A remote access server
- C) A proxy server
- D) Port scanning

Correct Answer: A
Explanation: An application-level gateway provides the most detailed and secure filtering by inspecting traffic at the application layer, which can protect against hacking attempts more effectively than the other options.

QUESTION 787
Which of the following is the MOST secure and economical method for connecting a private network over the Internet in a small- to medium-sized organization?

- A) **Virtual private network**
- B) Dedicated line
- C) Leased line
- D) Integrated services digital network (ISDN)

Correct Answer: A
Explanation: A Virtual Private Network (VPN) is the most secure and cost-effective solution, using encryption to secure data sent over public networks, while the other options are typically more expensive.

QUESTION 788
The potential for unauthorized system access by way of terminals or workstations within an organization's facility is increased when:

- A) **Connecting points are available in the facility to connect laptops to the network.**
- B) Users take precautions to keep their passwords confidential.
- C) Terminals with password protection are located in insecure locations.
- D) Terminals are located within the facility in small clusters under the supervision of an administrator.

Correct Answer: A
Explanation: Connecting points available in the facility can allow unauthorized individuals to connect to the network with a laptop, increasing the risk of unauthorized access.

QUESTION 789
Which of the following functions is performed by a virtual private network (VPN)?

- A) **Hiding information from sniffers on the net**
- B) Enforcing security policies
- C) Detecting misuse or mistakes
- D) Regulating access

Correct Answer: A
Explanation: A VPN encrypts traffic, hiding information from sniffers. It does not enforce policies, detect misuse, or regulate access directly, but provides secure communication.

QUESTION 790
Applying a digital signature to data traveling in a network provides:

- A) Confidentiality and integrity.
- B) Security and nonrepudiation.
- C) **Integrity and nonrepudiation.**
- D) Confidentiality and nonrepudiation.

Correct Answer: C
Explanation: A digital signature ensures integrity (the data has not been altered) and nonrepudiation (the sender cannot deny sending the message). It does not provide confidentiality, which requires encryption.

QUESTION 791
Which of the following would an IS auditor consider a weakness when performing an audit of an organization that uses a public key infrastructure (PKI) with digital certificates for its business-to-consumer transactions via the internet?

- A. Customers are widely dispersed geographically, but the certificate authorities are not.
- B. Customers can make their transactions from any computer or mobile device.
- C. The certificate authority has several data processing subcenters to administer certificates.
- D. The organization is the owner of the certificate authority.

Correct Answer: D
Explanation: If the organization is the owner of the certificate authority (CA), this could lead to a conflict of interest, potentially undermining the trustworthiness of the PKI. A CA should be a trusted third party to avoid any appearance of impropriety in generating certificates. The other options are not considered weaknesses.

QUESTION 792
Which of the following implementation modes would provide the GREATEST amount of security for outbound data connecting to the internet?

- A. Transport mode with authentication header (AH) plus encapsulating security payload (ESP)
- B. Secure Sockets Layer (SSL) mode
- C. Tunnel mode with AH plus ESP
- D. Triple-DES encryption mode

Correct Answer: C
Explanation: Tunnel mode with AH (Authentication Header) plus ESP (Encapsulating Security Payload) provides the greatest amount of security because it encrypts both the payload and the header, securing the entire data packet. This ensures confidentiality, integrity, and authenticity. Transport mode only protects the payload, while SSL and Triple-DES modes do not provide full protection of the packet.

QUESTION 793
Which of the following is the MOST reliable sender authentication method?

- A. Digital signatures
- B. Asymmetric cryptography
- C. Digital certificates
- D. Message authentication code (MAC)

Correct Answer: C
Explanation: Digital certificates are issued by a trusted third party (certificate authority) and provide the most reliable method for sender authentication. While digital signatures and asymmetric cryptography are also important for ensuring the authenticity of a message, digital certificates validate the sender's public key, ensuring that the sender is who they claim to be.

QUESTION 794
Which of the following provides the GREATEST assurance of message authenticity?

- A. The prehash code is derived mathematically from the message being sent.
- B. The prehash code is encrypted using the sender's private key.
- C. The prehash code and the message are encrypted using the secret key.
- D. The sender attains the recipient's public key and verifies the authenticity of its digital certificate with a certificate authority.

Correct Answer: B
Explanation: Encrypting the prehash code using the sender's private key provides the greatest assurance of message authenticity. It ensures that the message was not altered and can only be verified using the sender's public key, proving the message's origin and authenticity.

QUESTION 795

Which of the following internet security threats could compromise integrity?

- A. Theft of data from the client
- B. Exposure of network configuration information
- C. A Trojan horse browser
- D. Eavesdropping on the net

Correct Answer: C

Explanation: A Trojan horse browser can compromise the integrity of data by modifying it without the user's knowledge. Other options, such as data theft and eavesdropping, primarily compromise confidentiality.

QUESTION 796

Which of the following is a concern when data are transmitted through Secure Sockets Layer (SSL) encryption, implemented on a trading partner's server?

- A. The organization does not have control over encryption.
- B. Messages are subjected to wiretapping.
- C. Data might not reach the intended recipient.
- D. The communication may not be secure.

Correct Answer: A

Explanation: The primary concern with using SSL encryption on a trading partner's server is that the organization does not have control over the encryption process. The trading partner is responsible for encryption and decryption, which introduces potential risks. Wiretapping is not a concern since SSL encrypts the communication.

QUESTION 797

If inadequate, which of the following would be the MOST likely contributor to a denial-of-service (DoS) attack?

- A. Router configuration and rules
- B. Design of the internal network
- C. Updates to the router system software
- D. Audit testing and review techniques

Correct Answer: A

Explanation: Inadequate router configuration and rules could expose the network to denial-of-service (DoS) attacks. Routers control access to the network, and poor configuration could allow malicious traffic to flood the network. The other options are less likely to directly contribute to a DoS attack.

QUESTION 798

The Secure Sockets Layer (SSL) protocol addresses the confidentiality of a message through:

- A. symmetric encryption.
- B. message authentication code.
- C. hash function.
- D. digital signature certificates.

Correct Answer: A

Explanation: SSL ensures the confidentiality of a message through symmetric encryption. It uses symmetric keys to encrypt and decrypt data exchanged between a client and server. Message authentication codes and hash functions ensure integrity, while digital signature certificates ensure authenticity.

QUESTION 799

The PRIMARY goal of a web site certificate is:

- A. authentication of the web site that will be surfed.
- B. authentication of the user who surfs through that site.
- C. preventing surfing of the web site by hackers.
- D. the same purpose as that of a digital certificate.

Correct Answer: A
Explanation: The primary goal of a website certificate is to authenticate the website, ensuring the user that they are accessing a legitimate site. It does not authenticate users or prevent hackers from accessing the site.

QUESTION 800
An IS auditor performing detailed network assessments and access control reviews should FIRST:

- A. determine the points of entry.
- B. evaluate users' access authorization.
- C. assess users' identification and authorization.
- D. evaluate the domain-controlling server configuration.

Correct Answer: A
Explanation: When conducting network assessments and access control reviews, the IS auditor should first determine the points of entry into the system. Identifying the entry points helps ensure the appropriate controls are in place to protect the network from unauthorized access. Other steps, such as evaluating access authorization and reviewing server configurations, come later.