**QUESTION 601**
**Which of the following is widely accepted as one of the critical components in networking management?**
- Configuration management
- Topological mappings
- Application of monitoring tools
- Proxy server troubleshooting

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Configuration management is widely accepted as a key component in networking management. It deals with maintaining the network's structure, ensuring functionality, and monitoring performance. While topological mappings provide outlines of network connectivity, application monitoring and proxy server troubleshooting are not as integral to overall network management.

---

**QUESTION 602**
**Which of the following controls will MOST effectively detect the presence of bursts of errors in network transmissions?**
- Parity check
- Echo check
- Block sum check
- Cyclic redundancy check

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Cyclic redundancy check (CRC) is highly effective for detecting errors in network transmissions. CRC verifies blocks of data and can detect multiple errors within a transmission. Parity and echo checks are less effective for detecting bursts of errors.

---

**QUESTION 603**
**Which of the following types of firewalls provide the GREATEST degree and granularity of control?**
- Screening router
- Packet filter
- Application gateway
- Circuit gateway

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Application gateways offer the highest degree of control and granularity by inspecting the payload of packets, allowing for more detailed security decisions. In contrast, screening routers and packet filters operate primarily at the network layer, and circuit gateways establish connections but do not inspect content at the same level.

---

**QUESTION 604**
**Which of the following is MOST directly affected by network performance monitoring tools?**
- Integrity
- Availability
- Completeness
- Confidentiality

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**

Network performance monitoring tools are primarily concerned with availability, ensuring that the network remains operational. These tools help detect service disruptions but do not directly address data integrity, completeness, or confidentiality.

---

**QUESTION 605**

**A review of wide area network (WAN) usage discovers that traffic on one communication line between sites, synchronously linking the master and standby database, peaks at 96 percent of the line capacity. An IS auditor should conclude that:**

- Analysis is required to determine if a pattern emerges that results in a service loss for a short period of time.
- WAN capacity is adequate for the maximum traffic demands since saturation has not been reached.
- The line should immediately be replaced by one with a larger capacity to provide approximately 85 percent saturation.
- Users should be instructed to reduce their traffic demands or distribute them across all service hours to flatten bandwidth consumption.

**Correct Answer:** A

**Section:** IT SERVICE DELIVERY AND SUPPORT

**Explanation:**

Before recommending upgrades, the IS auditor should conduct an analysis to determine if high usage is consistent or an anomaly. If it is a regular occurrence, more capacity may be required. Occasional peaks do not justify immediate line replacement.

---

**QUESTION 606**

**While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:**

- Recommend the use of disk mirroring.
- Review the adequacy of offsite storage.
- Review the capacity management process.
- Recommend the use of a compression algorithm.

**Correct Answer:** C

**Section:** IT SERVICE DELIVERY AND SUPPORT

**Explanation:**

The IS auditor should focus on reviewing the capacity management process to ensure that resources are being used efficiently. This will help anticipate future needs and prevent overspending or resource shortages. Disk mirroring and compression may address storage issues but are not the primary focus in this scenario.

---

**QUESTION 607**

**In a small organization, an employee performs computer operations and, when the situation demands, program modifications. Which of the following should the IS auditor recommend?**

- Automated logging of changes to development libraries
- Additional staff to provide separation of duties
- Procedures that verify that only approved program changes are implemented
- Access controls to prevent the operator from making program modifications

**Correct Answer:** C

**Section:** IT SERVICE DELIVERY AND SUPPORT

**Explanation:**

In small organizations where segregation of duties may not be possible, compensating controls should be implemented. Verifying that only approved changes are made ensures accountability and security. While additional staff would be ideal, it may not be feasible.

---

**QUESTION 608**

**Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?**

- Assess the impact of patches prior to installation.
- Ask the vendors for a new software version with all fixes included.
- Install the security patch immediately.
- Decline to deal with these vendors in the future.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Before applying any patch, it is important to assess its impact on existing systems to avoid disrupting other functionalities. Installing patches immediately without proper testing could introduce new issues. Seeking a full software version or avoiding the vendor is not practical in most cases.

---

**QUESTION 609**
**Which of the following controls would be MOST effective in ensuring that production source code and object code are synchronized?**

- Release-to-release source and object comparison reports
- Library control software restricting changes to source code
- Restricted access to source code and object code
- Date and time-stamp reviews of source and object code

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Date and time-stamp reviews ensure that the source and object code are synchronized after compilation. This is the most reliable way to verify that the production object code matches the approved source code.

**QUESTION 610**
**Change management procedures are established by IS management to:**

- Control the movement of applications from the test environment to the production environment.
- Control the interruption of business operations from lack of attention to unresolved problems.
- Ensure the uninterrupted operation of the business in the event of a disaster.
- Verify that system changes are properly documented.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Change management procedures are primarily established to control the migration of applications from the test to production environment. They ensure that only tested and approved applications are deployed, minimizing risks to business operations.

---

**QUESTION 611**
**In regard to moving an application program from the test environment to the production environment, the BEST control would be to have the:**

- Application programmer copy the source program and compiled object module to the production libraries.
- Application programmer copy the source program to the production libraries and then have the production control group compile the program.
- Production control group compile the object module to the production libraries using the source program in the test environment.
- Production control group copy the source program to the production libraries and then compile the program.

**Correct Answer:** D

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The best control involves having the production control group copy the source program to the production libraries and compile it. This reduces the risk of unauthorized changes being introduced into the production environment.

---

**QUESTION 612**
**An IS auditor reviewing database controls discovered that changes to the database during normal working hours were handled through a standard set of procedures. However, changes made after normal hours required only an abbreviated number of steps. In this situation, which of the following would be considered an adequate set of compensating controls?**

- Allow changes to be made only with the DBA user account.
- Make changes to the database after granting access to a normal user account.
- Use the DBA user account to make changes, log the changes, and review the change log the following day.
- Use the normal user account to make changes, log the changes, and review the change log the following day.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Using the DBA account for changes, logging the changes, and reviewing the log the next day is an effective compensating control. It allows monitoring of changes made outside of normal hours, reducing the risk of unauthorized modifications.

---

**QUESTION 613**
**Which of the following tests performed by an IS auditor would be the MOST effective in determining compliance with an organization's change control procedures?**

- Review software migration records and verify approvals.
- Identify changes that have occurred and verify approvals.
- Review change control documentation and verify approvals.
- Ensure that only appropriate staff can migrate changes into production.

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Identifying actual changes and verifying their approvals is the most effective way to determine compliance with change control procedures. This method checks what has occurred, as opposed to only reviewing records or documentation.

---

**QUESTION 614**
**An IS auditor reviewing a database application discovers that the current configuration does not match the originally designed structure. Which of the following should be the IS auditor's next action?**

- Analyze the need for the structural change.
- Recommend restoration to the originally designed structure.
- Recommend the implementation of a change control process.
- Determine if the modifications were properly approved.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The IS auditor's next step should be to determine if the modifications were properly approved. This ensures that any changes to the database configuration were authorized, preventing unauthorized alterations.

**QUESTION 615**
**A programmer maliciously modified a production program to change data and then restored the original code. Which of the following would MOST effectively detect the malicious activity?**
- Comparing source code
- Reviewing system log files
- Comparing object code
- Reviewing executable and source code integrity

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Reviewing system log files is the best method to detect malicious activity, as they provide a record of actions performed in the system. Comparing code is ineffective if the original code is restored, and integrity checks wouldn't reveal past malicious actions.

**QUESTION 616**
**The purpose of code signing is to provide assurance that:**
- The software has not been subsequently modified.
- The application can safely interface with another signed application.
- The signer of the application is trusted.
- The private key of the signer has not been compromised.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Code signing ensures that the executable code has not been modified after being signed. The other options describe potential weaknesses of code signing or other security concerns unrelated to its primary purpose.

**QUESTION 617**
**An IS auditor should recommend the use of library control software to provide reasonable assurance that:**
- Program changes have been authorized.
- Only thoroughly tested programs are released.
- Modified programs are automatically moved to production.
- Source and executable code integrity is maintained.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Library control software is primarily used to ensure that program changes are authorized before they are moved to production. While it can provide assurance for some aspects of source and executable code integrity, its main function is controlling changes.

**QUESTION 618**
**An organization has recently installed a security patch, which crashed the production server. To minimize the probability of this occurring again, an IS auditor should:**
- Apply the patch according to the patch's release notes.
- Ensure that a good change management process is in place.
- Thoroughly test the patch before sending it to production.
- Approve the patch after doing a risk assessment.

**Correct Answer:** B

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The IS auditor should focus on ensuring that a good change management process is in place, which includes proper testing and risk assessment of patches. Testing patches before production is a part of this overall process, but the change management process is key to preventing future issues.

---

**QUESTION 619**
**When reviewing procedures for emergency changes to programs, the IS auditor should verify that the procedures:**

- Allow changes, which will be completed using after-the-fact follow-up.
- Allow undocumented changes directly to the production library.
- Do not allow any emergency changes.
- Allow programmers permanent access to production programs.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Emergency changes should be allowed but completed with after-the-fact follow-up to ensure proper documentation and review. This allows for quick fixes while maintaining control over production environments.

---

**QUESTION 620**
**To determine if unauthorized changes have been made to production code the BEST audit procedure is to:**

- Examine the change control system records and trace them forward to object code files.
- Review access control permissions operating within the production program libraries.
- Examine object code to find instances of changes and trace them back to change control records.
- Review change approved designations established within the change control system.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Examining object code to identify changes and tracing them back to change control records is the best way to determine if unauthorized changes have been made. This provides a direct check of the actual production environment.

---

**QUESTION 621**
**The application systems of an organization using open-source software have no single recognized developer producing patches. Which of the following would be the MOST secure way of updating open-source software?**

- Rewrite the patches and apply them.
- Code review and application of available patches.
- Develop in-house patches.
- Identify and test suitable patches before applying them.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The most secure approach is to identify and test suitable patches before applying them. This reduces the risk of applying faulty or malicious patches.

---

**QUESTION 622**
**An IS auditor discovers that developers have operator access to the command line of a production environment operating system. Which of the following controls would BEST mitigate the risk of undetected and unauthorized program changes to the production environment?**

- Commands typed on the command line are logged.
- Hash keys are calculated periodically for programs and matched against hash keys calculated for the most recent authorized versions of the programs.
- Access to the operating system command line is granted through an access restriction tool with preapproved rights.
- Software development tools and compilers have been removed from the production environment.

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Periodic calculation of hash keys for programs and matching them against the most recent authorized versions ensures the detection of unauthorized changes. Logs and access restriction tools can help, but they don't directly address unauthorized changes.

---

**QUESTION 623**
**Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?**

- Change management.
- Backup and recovery.
- Incident management.
- Configuration management.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Configuration management includes tools and processes for recording baselines of software releases. These baselines can be used as a point of reference if issues arise in future releases.

---

**QUESTION 624**
**An IS auditor notes that patches for the operating system used by an organization are deployed by the IT department as advised by the vendor. The MOST significant concern an IS auditor should have with this practice is the nonconsideration by IT of:**

- The training needs for users after applying the patch.
- Any beneficial impact of the patch on the operational systems.
- Delaying deployment until testing the impact of the patch.
- The necessity of advising end users of new patches.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The most significant concern is the lack of testing. Applying patches without testing risks system disruption. Training users or advising them of patches is less critical than preventing system outages.

---

**QUESTION 625**
**In a small organization, developers may release emergency changes directly to production. Which of the following will BEST control the risk in this situation?**

- Approve and document the change the next business day.
- Limit developer access to production to a specific timeframe.
- Obtain secondary approval before releasing to production.
- Disable the compiler option in the production machine.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
In emergency situations, allowing developers to release changes directly can be acceptable as long as the change is documented and approved retroactively. Limiting access to timeframes or requiring secondary approval can hinder timely fixes.

**QUESTION 626**
**Time constraints and expanded needs have been found by an IS auditor to be the root causes for recent violations of corporate data definition standards in a new business intelligence project. Which of the following is the MOST appropriate suggestion for an auditor to make?**

- Achieve standards alignment through an increase of resources devoted to the project.
- Align the data definition standards after completion of the project.
- Delay the project until compliance with standards can be achieved.
- Enforce standard compliance by adopting punitive measures against violators.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The best suggestion is to increase resources to ensure compliance with standards. Delaying the project or enforcing punitive measures could impact project success, while aligning standards post-project poses risks to consistency and quality.

---

**QUESTION 627**
**After installing a network, an organization installed a vulnerability assessment tool or security scanner to identify possible weaknesses. Which is the MOST serious risk associated with such tools?**

- Differential reporting.
- False-positive reporting.
- False-negative reporting.
- Less-detail reporting.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
False-negative reporting is the most serious risk because it means vulnerabilities could go undetected and unaddressed. While false positives are also a concern, they at least prompt further investigation, whereas false negatives leave the system exposed.

---

**QUESTION 628**
**The FIRST step in managing the risk of a cyber attack is to:**

- Assess the vulnerability impact.
- Evaluate the likelihood of threats.
- Identify critical information assets.
- Estimate potential damage.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The first step in managing risk is identifying and classifying critical information assets. This allows for prioritization of protective measures based on the value and sensitivity of these assets. Threat evaluation and impact assessment follow this step.

---

**QUESTION 629**
**Which of the following is the MOST effective method for dealing with the spreading of a network worm that exploits a vulnerability in a protocol?**

- Install the vendor's security fix for the vulnerability.
- Block the protocol traffic in the perimeter firewall.
- Block the protocol traffic between internal network segments.
- Stop the service until an appropriate security fix is installed.

**Correct Answer:** D

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Stopping the vulnerable service and then applying the appropriate security fix is the most effective method to prevent a network worm from spreading. Simply blocking traffic or installing fixes while the service is still running may not fully stop the worm's propagation.

---

**QUESTION 630**
**The PRIMARY objective of performing a post-incident review is that it presents an opportunity to:**

- Improve internal control procedures.
- Harden the network to industry best practices.
- Highlight the importance of incident response management to management.
- Improve employee awareness of the incident response process.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The main goal of a post-incident review is to improve internal control procedures by learning from the incident. This process helps to prevent future incidents and strengthen the organization's overall security posture.

**QUESTION 631**
The computer security incident response team (CSIRT) of an organization disseminates detailed descriptions of recent threats. An IS auditor's GREATEST concern should be that the users might:

- Use this information to launch attacks.
- Forward the security alert.
- Implement individual solutions.
- Fail to understand the threat.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
An organization's CSIRT should disseminate recent threats to assist users in understanding security risks. However, this poses the risk that users might misuse the information to launch attacks. Forwarding alerts is generally harmless, implementing individual solutions is unlikely to happen, and failing to understand the threat is not as critical a concern.

---

**QUESTION 632**
The MAIN criterion for determining the severity level of a service disruption incident is:

- Cost of recovery.
- Negative public opinion.
- Geographic location.
- Downtime.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The longer the downtime, the greater the severity of the incident. Cost of recovery may be minimal, yet downtime can have a significant impact. Negative public opinion is a symptom, and geographic location does not affect severity.

---

**QUESTION 633**
Which of the following would be an indicator of the effectiveness of a computer security incident response team?

- Financial impact per security incident.

- Number of security vulnerabilities that were patched.
- Percentage of business applications that are being protected.
- Number of successful penetration tests.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The financial impact per security incident is the most important indicator of effectiveness. While the other options measure aspects of security, they do not directly indicate the response team's effectiveness.

---

**QUESTION 634**
An IS auditor evaluating the resilience of a high-availability network should be MOST concerned if:

- The setup is geographically dispersed.
- The network servers are clustered in a site.
- A hot site is ready for activation.
- Diverse routing is implemented for the network.

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Clustering servers in one location poses a risk to the entire network if that site experiences a disaster, creating a single point of failure. Geographical dispersion and diverse routing provide alternative options.

---

**QUESTION 635**
Which of the following network components is PRIMARILY set up to serve as a security measure by preventing unauthorized traffic between different segments of the network?

- Firewalls
- Routers
- Layer 2 switches
- VLANs

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Firewalls are the primary tools to prevent unauthorized access between network segments, while routers and switches have different functionalities regarding packet handling and traffic segregation.

---

**QUESTION 636**
A company is implementing a dynamic host configuration protocol (DHCP). Given that the following conditions exist, which represents the GREATEST concern?

- Most employees use laptops.
- A packet filtering firewall is used.
- The IP address space is smaller than the number of PCs.
- Access to a network port is not restricted.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Unrestricted access to network ports allows anyone to connect to the internal network, posing significant security risks. The other conditions, while concerning, do not present the same level of exposure.

---

**QUESTION 637**
An IS auditor is performing a network security review of a telecom company that provides Internet connection services to shopping malls for their wireless customers. The company uses Wireless Transport Layer Security (WTLS) and Secure Sockets Layer (SSL) technology for protecting their customer's payment information. The IS auditor should be MOST concerned if a hacker:

- Compromises the Wireless Application Protocol (WAP) gateway.

- Installs a sniffing program in front of the server.
- Steals a customer's PDA.
- Listens to the wireless transmission.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
If the WAP gateway is compromised, encrypted messages must be decrypted for transmission, exposing them to potential interception. Other options present risks but do not compromise the security of all messages.

---

**QUESTION 638**
Which of the following BEST reduces the ability of one device to capture the packets that are meant for another device?

- Filters
- Switches
- Routers
- Firewalls

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Switches transmit packets specifically to the intended devices, minimizing the risk of interception by other devices on the network.

---

**QUESTION 639**
In a client-server system, which of the following control techniques is used to inspect activity from known or unknown users?

- Diskless workstations
- Data encryption techniques
- Network monitoring devices
- Authentication systems

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Network monitoring devices inspect traffic and can identify client addresses, serving as a detective control for unauthorized access.

---

**QUESTION 640**
When reviewing system parameters, an IS auditor's PRIMARY concern should be that:

- They are set to meet security and performance requirements.
- Changes are recorded in an audit trail and periodically reviewed.
- Changes are authorized and supported by appropriate documents.
- Access to parameters in the system is restricted.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The primary concern should be ensuring parameters meet security and performance requirements, as improper settings can negate the effectiveness of other controls.

---

**QUESTION 641**
Which of the following is a control over component communication failure/errors?

- Restricting operator access and maintaining audit trails
- Monitoring and reviewing system engineering activity
- Providing network redundancy

- Establishing physical barriers to the data transmitted over the network

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Network redundancy helps prevent communication failures by providing alternative paths for data transmission.

---

**QUESTION 642**
An installed Ethernet cable run in an unshielded twisted pair (UTP) network is more than 100 meters long. Which of the following could be caused by the length of the cable?

- Electromagnetic interference (EMI)
- Cross-talk
- Dispersion
- Attenuation

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Attenuation is the weakening of signals over distance, which can lead to communication problems in a UTP network.

---

**QUESTION 643**
Which of the following line media would provide the BEST security for a telecommunication network?

- Broadband network digital transmission
- Baseband network
- Dial-up
- Dedicated lines

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Dedicated lines are not shared, reducing the risk of interception and ensuring better security.

---

**QUESTION 644**
Which of the following types of firewalls would BEST protect a network from an internet attack?

- Screened subnet firewall
- Application filtering gateway
- Packet filtering router
- Circuit-level gateway

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
A screened subnet firewall provides comprehensive security by filtering traffic based on multiple criteria.

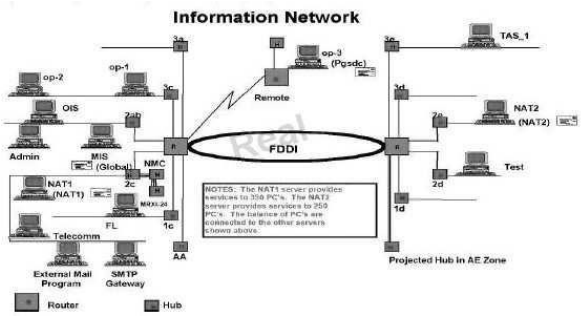
---

**QUESTION 645**
Neural networks are effective in detecting fraud because they can:

- Discover new trends since they are inherently linear.
- Solve problems where large and general sets of training data are not obtainable.
- Attack problems that require consideration of a large number of input variables.
- Make assumptions about the shape of any curve relating variables to the output.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Neural networks excel at processing complex relationships with numerous variables, making them effective for fraud detection.

**QUESTION 646**



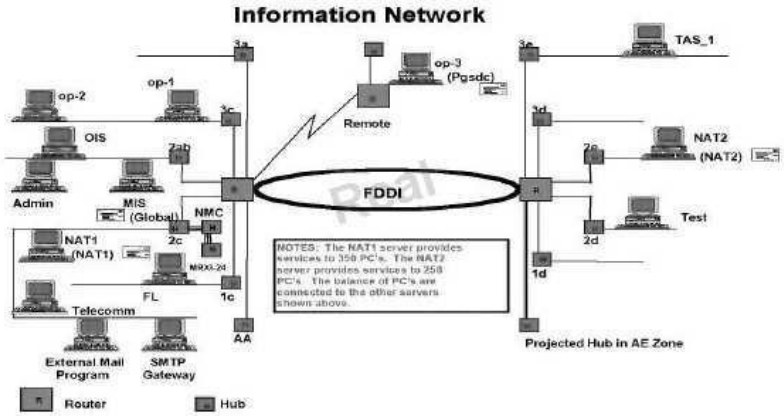

Assuming this diagram represents an internal facility and the organization is implementing a firewall protection program, where should firewalls be installed?

- No firewalls are needed
- Op-3 location only
- MIS (Global) and NAT2
- SMTP Gateway and op-3

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The objective of a firewall is to protect a trusted network from an untrusted network; therefore, firewalls should be installed at locations with external connections. All other answers are either incomplete or refer to internal connections.

---

**QUESTION 647**

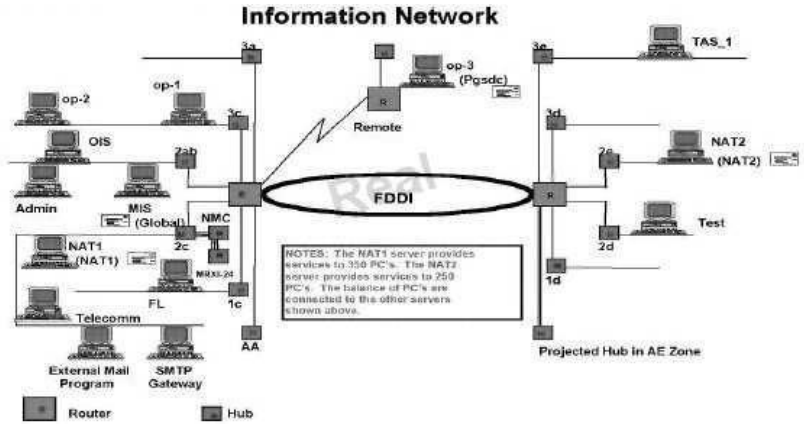



For locations 3a, 1d, and 3d, the diagram indicates hubs with lines that appear to be open and active. Assuming that is true, what control, if any, should be recommended to mitigate this weakness?

- Intelligent hub
- Physical security over the hubs
- Physical security and an intelligent hub
- No controls are necessary since this is not a weakness

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Open hubs represent a significant control weakness because they allow easy access to the network. An intelligent hub would enable the deactivation of individual ports while keeping others active. Additionally, physical security would enhance protection over the active hubs.

**QUESTION 648**




In the 2c area of the diagram, there are three hubs connected to each other. What potential risk might this indicate?

- Virus attack
- Performance degradation
- Poor management controls
- Vulnerability to external hackers

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Hubs are internal devices typically without direct external connectivity, making them less vulnerable to hackers. While this may indicate poor management controls, the practice of stacking hubs likely leads to performance degradation.

---

**QUESTION 649**
An organization provides information to its supply chain partners and customers through an extranet infrastructure. Which of the following should be the GREATEST concern to an IS auditor reviewing the firewall security architecture?

- A Secure Sockets Layer (SSL) has been implemented for user authentication and remote administration of the firewall.
- Firewall policies are updated based on changing requirements.
- Inbound traffic is blocked unless the traffic type and connections have been specifically permitted.
- The firewall is placed on top of the commercial operating system with all installation options.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The greatest concern when implementing firewalls on commercial operating systems is the potential vulnerabilities that could compromise the firewall's security. Many breaches occur due to vulnerabilities in the underlying OS. Other options are essential practices for maintaining firewall security.

---

**QUESTION 650**
In a client-server architecture, a domain name service (DNS) is MOST important because it provides the:

- Address of the domain server.
- Resolution service for the name/address.
- IP addresses for the Internet.
- Domain name system.

**Correct Answer:** B

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
DNS primarily resolves domain names to IP addresses, enabling easier navigation of the Internet. It translates user-friendly names into the numeric IP addresses used for routing traffic.

---

**QUESTION 651**
In what way is a common gateway interface (CGI) MOST often used on a web server?

- Consistent way for transferring data to the application program and back to the user
- Computer graphics imaging method for movies and TV
- Graphic user interface for web design
- Interface to access the private gateway domain

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The common gateway interface (CGI) is a standard for passing user requests to application programs and returning data. It facilitates communication between the web server and applications, especially for form submissions.

---

**QUESTION 652**
Receiving an EDI transaction and passing it through the communication's interface stage usually requires:

- Translating and unbundling transactions.
- Routing verification procedures.
- Passing data to the appropriate application system.
- Creating a point of receipt audit log.

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The communication's interface stage necessitates routing verification procedures to ensure EDI transactions are correctly processed. Other options, while important, do not directly pertain to this stage.

---

**QUESTION 653**
Which of the following would be considered an essential feature of a network management system?

- A graphical interface to map the network topology
- Capacity to interact with the Internet to solve problems
- Connectivity to a help desk for advice on difficult issues
- An export facility for piping data to spreadsheets

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
A graphical interface for mapping the network topology is essential for effective network management. Other options may be useful but are not fundamental features of a network management system.

---

**QUESTION 654**
The most likely error to occur when implementing a firewall is:

- Incorrectly configuring the access lists.
- Compromising the passwords due to social engineering.
- Connecting a modem to the computers in the network.
- Inadequately protecting the network and server from virus attacks.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Errors in configuring access lists present significant challenges during firewall implementation, leading to

the highest likelihood of mistakes. Other options do not apply directly to the initial installation phase of a firewall.

---

**QUESTION 655**
When reviewing the implementation of a LAN, an IS auditor should FIRST review the:
- Node list.
- Acceptance test report.
- Network diagram.
- User's list.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
To effectively review a LAN implementation, an IS auditor should first examine the network diagram to confirm the system's structure and design, followed by other elements like the node list and acceptance test report.

**QUESTION 656**
Which of the following would be the MOST secure firewall system?
- Screened-host firewall
- Screened-subnet firewall
- Dual-homed firewall
- Stateful-inspection firewall

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
A screened-subnet firewall, also known as a demilitarized zone (DMZ), utilizes two packet filtering routers and a bastion host. This setup provides the most secure firewall system by supporting both network- and application-level security while defining a separate DMZ network.

---

**QUESTION 657**
Reconfiguring which of the following firewall types will prevent inward downloading of files through the File Transfer Protocol (FTP)?
- Circuit gateway
- Application gateway
- Packet filter
- Screening router

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
An application gateway firewall effectively prevents specific applications, such as FTP, from entering the organization's network. In contrast, a circuit gateway firewall prevents paths or circuits, not specific applications, from entering the network.

---

**QUESTION 658**
Which of the following applet intrusion issues poses the GREATEST risk of disruption to an organization?
- A program that deposits a virus on a client machine
- Applets recording keystrokes and, therefore, passwords
- Downloaded code that reads files on a client's hard drive
- Applets opening connections from the client machine

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**

Applet intrusion that opens connections from the client machine to other machines on the network poses the greatest risk, potentially leading to denial-of-service attacks and significant disruption of business continuity.

---

**QUESTION 659**
Which of the following protocols would be involved in the implementation of a router and an interconnectivity device monitoring system?

- Simple Network Management Protocol
- File Transfer Protocol
- Simple Mail Transfer Protocol
- Telnet

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The Simple Network Management Protocol (SNMP) provides a means to monitor and control network devices, making it essential for managing configurations and performance.

---

**QUESTION 660**
Java applets and ActiveX controls are distributed executable programs that execute in the background of a web browser client. This practice is considered reasonable when:

- a firewall exists.
- a secure web connection is used.
- the source of the executable file is certain.
- the host web site is part of the organization.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Acceptance of these executable files should be based on established trust. Knowing the source of the executable file allows for reasonable security, as opposed to relying solely on external defenses like firewalls or secure connections.

---

**QUESTION 661**
In large corporate networks having supply partners across the globe, network traffic may continue to rise. The infrastructure components in such environments should be scalable. Which of the following firewall architectures limits future scalability?

- Appliances
- Operating system-based
- Host-based
- Demilitarized

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Firewalls built as appliances have their software embedded in chips, making them less scalable since they cannot be moved to higher capacity servers. In contrast, firewalls based on operating systems or host-based solutions can be scaled more easily.

---

**QUESTION 662**
Which of the following types of transmission media provide the BEST security against unauthorized access?

- Copper wire
- Twisted pair
- Fiberoptic cables
- Coaxial cables

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Fiberoptic cables are significantly more secure than other transmission media, as they are less susceptible to unauthorized access compared to copper or coaxial cables.

---

**QUESTION 663**
Which of the following is the BEST audit procedure to determine if a firewall is configured in compliance with an organization's security policy?

- Review the parameter settings.
- Interview the firewall administrator.
- Review the actual procedures.
- Review the device's log file for recent attacks.

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Reviewing the parameter settings provides a strong basis for comparing the firewall's actual configuration to the security policy, offering solid audit evidence.

---

**QUESTION 664**
To determine how data are accessed across different platforms in a heterogeneous environment, an IS auditor should FIRST review:

- Business software.
- Infrastructure platform tools.
- Application services.
- System development tools.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Application services help isolate system developers from the complexities of IT infrastructure, allowing for a clearer understanding of data access across different platforms.

---

**QUESTION 665**
During the requirements definition phase for a database application, performance is listed as a top priority. To access the DBMS files, which of the following technologies should be recommended for optimal I/O performance?

- Storage area network (SAN)
- Network Attached Storage (NAS)
- Network file system (NFS v2)
- Common Internet File System (CIFS)

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
A Storage Area Network (SAN) provides optimal performance by allowing direct access to data stored on storage devices, making it similar to direct attached storage.

---

**QUESTION 666**
Reverse proxy technology for web servers should be deployed if:

- HTTP servers' addresses must be hidden.
- Accelerated access to all published pages is required.
- Caching is needed for fault tolerance.
- Bandwidth to the user is limited.

**Correct Answer:** A

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Reverse proxies are primarily designed to hide internal structures from outside access, ensuring that server addresses are not disclosed.

---

**QUESTION 667**
When auditing a proxy-based firewall, an IS auditor should:
- Verify that the firewall is not dropping any forwarded packets.
- Review Address Resolution Protocol (ARP) tables for appropriate mapping between media access control (MAC) and IP addresses.
- Verify that the filters applied to services such as HTTP are effective.
- Test whether routing information is forwarded by the firewall.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
A proxy-based firewall acts as an intermediary and does not forward packets, so verifying the effectiveness of the applied filters is crucial.

---

**QUESTION 668**
An IS auditor should review the configuration of which of the following protocols to detect unauthorized mappings between the IP address and the media access control (MAC) address?
- Simple Object Access Protocol (SOAP)
- Address Resolution Protocol (ARP)
- Routing Information Protocol (RIP)
- Transmission Control Protocol (TCP)

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
The Address Resolution Protocol (ARP) provides dynamic mapping between IP addresses and MAC addresses, making it essential for detecting unauthorized mappings.

---

**QUESTION 669**
An IS auditor examining the configuration of an operating system to verify the controls should review the:
- Transaction logs.
- Authorization tables.
- Parameter settings.
- Routing tables.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Parameter settings are crucial for determining how a system runs, and improper implementation can lead to unauthorized access and data corruption.

---

**QUESTION 670**
When reviewing an implementation of a VoIP system over a corporate WAN, an IS auditor should expect to find:
- An integrated services digital network (ISDN) data link.
- Traffic engineering.
- Wired equivalent privacy (WEP) encryption of data.
- Analog phone terminals.

**Correct Answer:** B

**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Traffic engineering is necessary to manage network performance and ensure quality of service for VoIP over a WAN, protecting it from packet loss and latency.

**QUESTION 671**
Which of the following is a feature of Wi-Fi Protected Access (WPA) in wireless networks?
- Session keys are dynamic
- Private symmetric keys are used
- Keys are static and shared
- Source addresses are not encrypted or authenticated

**Correct Answer:** A
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
WPA uses dynamic session keys, achieving stronger encryption than Wired Equivalent Privacy (WEP), which operates with static keys (the same key is used for everyone in the wireless network). All other choices are weaknesses of WEP.

---

**QUESTION 672**
During the audit of a database server, which of the following would be considered the GREATEST exposure?
- The password does not expire on the administrator account
- Default global security settings for the database remain unchanged
- Old data have not been purged
- Database activity is not fully logged

**Correct Answer:** B
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Default security settings for the database could allow issues like blank user passwords or passwords that were the same as the username. Logging all database activity is not practical. Failure to purge old data may present a performance issue but is not an immediate security concern. Choice A is an exposure but not as serious as B.

---

**QUESTION 673**
Which significant risk is introduced by running the file transfer protocol (FTP) service on a server in a demilitarized zone (DMZ)?
- A user from within could send a file to an unauthorized person.
- FTP services could allow a user to download files from unauthorized sources.
- A hacker may be able to use the FTP service to bypass the firewall.
- FTP could significantly reduce the performance of a DMZ server.

**Correct Answer:** C
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
Since FTP is considered an insecure protocol, it should not be installed on a server in a DMZ. FTP could allow an unauthorized user to gain access to the network. Sending files to an unauthorized person and the risk of downloading unauthorized files are not as significant as having a firewall breach. The presence of the utility does not reduce the performance of a DMZ server; therefore, performance degradation is not a threat.

---

**QUESTION 674**
The MAIN reason for requiring that all computer clocks across an organization be synchronized is to:

- Prevent omission or duplication of transactions.
- Ensure smooth data transition from client machines to servers.
- Ensure that e-mail messages have accurate time stamps.
- Support the incident investigation process.

**Correct Answer:** D
**Section:** IT SERVICE DELIVERY AND SUPPORT
**Explanation:**
During an investigation of incidents, audit logs are used as evidence, and the time stamp information in them is useful. If the clocks are not synchronized, investigations will be more difficult because a timeline of events might not be easily established. Time-stamping a transaction has nothing to do with the update itself. Therefore, the possibility of omission or duplication of transactions does not exist. Data transfer has nothing to do with the timestamp. While the timestamp on an email may not be accurate, this is not a significant issue.

---

**QUESTION 675**
When reviewing the configuration of network devices, an IS auditor should FIRST identify:
- The best practices for the type of network devices deployed.
- Whether components of the network are missing.
- The importance of the network device in the topology.
- Whether subcomponents of the network are being used appropriately.

**Correct Answer:** C
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The first step is to understand the importance and role of the network device within the organization's network topology. After understanding the devices in the network, the best practice for using the device should be reviewed to ensure that there are no anomalies within the configuration. Identification of which component or subcomponent is missing or being used inappropriately can only be known upon reviewing and understanding the topology and the best practice for the deployment of the device in the network.

---

**QUESTION 676**
Which of the following functions should be performed by the application owners to ensure an adequate segregation of duties between IS and end users?
- System analysis
- Authorization of access to data
- Application programming
- Data administration

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The application owner is responsible for authorizing access to data. Application development and programming are functions of the IS department. Similarly, system analysis should be performed by qualified persons in IS who have knowledge of IS and user requirements. Data administration is a specialized function related to database management systems and should be performed by qualified database administrators.

---

**QUESTION 677**
Accountability for the maintenance of appropriate security measures over information assets resides with the:
- Security administrator.
- Systems administrator.
- Data and systems owners.
- Systems operations group.

**Correct Answer:** C

**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Management should ensure that all information assets (data and systems) have an appointed owner who makes decisions about classification and access rights. System owners typically delegate day-to-day custodianship to the systems delivery/operations group and security responsibilities to a security administrator. Owners, however, remain accountable for the maintenance of appropriate security measures.

---

**QUESTION 678**
The GREATEST risk when end users have access to a database at its system level, instead of through the application, is that the users can:

- Make unauthorized changes to the database directly, without an audit trail.
- Make use of a system query language (SQL) to access information.
- Remotely access the database.
- Update data without authentication.

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Having access to the database could provide access to database utilities, which can update the database without an audit trail and without using the application. Using SQL only provides read access to information; in a networked environment, accessing the database remotely does not make a difference. What is critical is what is possible or completed through this access. To access a database, it is necessary that a user is authenticated using a user ID.

---

**QUESTION 679**
To determine who has been given permission to use a particular system resource, an IS auditor should review:

- Activity lists.
- Access control lists.
- Logon ID lists.
- Password lists.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Access control lists are the authorization tables that document the users who have been given permission to use a particular system resource and the types of access they have been granted. The other choices would not document who has been given permission to use (access) specific system resources.

---

**QUESTION 680**
Which of the following is the MOST effective control when granting temporary access to vendors?

- Vendor access corresponds to the service level agreement (SLA).
- User accounts are created with expiration dates and are based on services provided.
- Administrator access is provided for a limited period.
- User IDs are deleted when the work is completed.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The most effective control is to ensure that the granting of temporary access is based on services to be provided and that there is an expiration date (hopefully automated) associated with each ID. The SLA may have a provision for providing access, but this is not a control; it would merely define the need for access. Vendors require access for a limited period during the time of service. However, it is important to ensure that the access during this period is monitored. Deleting these user IDs after the work is completed is necessary, but if not automated, the deletion could be overlooked.

**QUESTION 681**
During a logical access controls review, an IS auditor observes that user accounts are shared. The GREATEST risk resulting from this situation is that:
- An unauthorized user may use the ID to gain access.
- User access management is time-consuming.
- Passwords are easily guessed.
- User accountability may not be established.

**Correct Answer:** D
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The use of a single user ID by more than one individual precludes knowing who, in fact, used that ID to access a system; therefore, it is literally impossible to hold anyone accountable. All user IDs, not just shared IDs, can be used by unauthorized individuals. Access management would not be any different with shared IDs, and shared user IDs do not necessarily have easily guessed passwords.

---

**QUESTION 682**
Which of the following satisfies a two-factor user authentication?
- Iris scanning plus fingerprint scanning
- Terminal ID plus global positioning system (GPS)
- A smart card requiring the user's PIN
- User ID along with password

**Correct Answer:** C
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
A smart card addresses what the user has. This is generally used in conjunction with testing what the user knows, e.g., a keyboard password or personal identification number (PIN). Proving who the user is usually requires a biometrics method, such as fingerprint, iris scan, or voice verification, to prove biology. This is not a two-factor user authentication, because it proves only who the user is. A global positioning system (GPS) receiver reports on where the user is. The use of an ID and password (what the user knows) is a single-factor user authentication.

---

**QUESTION 683**
What is the MOST effective method of preventing unauthorized use of data files?
- Automated file entry
- Tape librarian
- Access control software
- Locked library

**Correct Answer:** C
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Access control software is an active control designed to prevent unauthorized access to data.

---

**QUESTION 684**
Which of the following is the PRIMARY safeguard for securing software and data within an information processing facility?
- Security awareness
- Reading the security policy
- Security committee
- Logical access controls

**Correct Answer:** D
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**

To retain a competitive advantage and meet basic business requirements, organizations must ensure that the integrity of the information stored on their computer systems preserves the confidentiality of sensitive data and ensures the continued availability of their information systems. To meet these goals, logical access controls must be in place. Awareness (choice A) itself does not protect against unauthorized access or disclosure of information. Knowledge of an information systems security policy (choice B), which should be known by the organization's employees, would help to protect information, but would not prevent unauthorized access. A security committee (choice C) is key to the protection of information assets, but would address security issues from a broader perspective.

---

**QUESTION 685**
Which of the following is a benefit of using a callback device?

- Provides an audit trail
- Can be used in a switchboard environment
- Permits unlimited user mobility
- Allows call forwarding

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
A callback feature hooks into the access control software and logs all authorized and unauthorized access attempts, permitting follow-up and further review of potential breaches. Call forwarding (choice D) is a means of potentially bypassing callback control. By dialing through an authorized phone number from an unauthorized phone number, a perpetrator can gain computer access. This vulnerability can be controlled through callback systems that are available.

**QUESTION 686**
When reviewing an organization's logical access security, which of the following should be of MOST concern to an IS auditor?

- Passwords are not shared.
- Password files are not encrypted.
- Redundant logon IDs are deleted.
- The allocation of logon IDs is controlled.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
When evaluating the technical aspects of logical security, unencrypted files represent the greatest risk. The sharing of passwords, checking for the redundancy of logon IDs, and proper logon ID procedures are essential, but they are less important than ensuring that the password files are encrypted.

---

**QUESTION 687**
Passwords should be:

- Assigned by the security administrator for first time logon.
- Changed every 30 days at the discretion of the user.
- Reused often to ensure the user does not forget the password.
- Displayed on the screen so that the user can ensure that it has been entered properly.

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Initial password assignment should be done discretely by the security administrator. Passwords should be changed often (e.g., every 30 days); however, changing should not be voluntary, it should be required by the system. Systems should not permit previous passwords to be used again. Old passwords may have been compromised and would thus permit unauthorized access. Passwords should not be displayed in any form.

**QUESTION 688**
When performing an audit of access rights, an IS auditor should be suspicious of which of the following if allocated to a computer operator?
- Read access to data
- Delete access to transaction data files
- Logged read/execute access to programs
- Update access to job control language/script files

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Deletion of transaction data files should be a function of the application support team, not operations staff. Read access to production data is a normal requirement of a computer operator, as is logged access to programs and access to JCL to control job execution.

---

**QUESTION 689**
To prevent unauthorized entry to the data maintained in a dial-up, fast response system, an IS auditor should recommend:
- Online terminals are placed in restricted areas.
- Online terminals are equipped with key locks.
- ID cards are required to gain access to online terminals.
- Online access is terminated after a specified number of unsuccessful attempts.

**Correct Answer:** D
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The most appropriate control to prevent unauthorized entry is to terminate connection after a specified number of attempts. This will deter access through guessing of IDs and passwords. The other choices are physical controls, which are not effective in deterring unauthorized accesses via telephone lines.

---

**QUESTION 690**
An IS auditor conducting an access control review in a client-server environment discovers that all printing options are accessible by all users. In this situation, the IS auditor is MOST likely to conclude that:
- Exposure is greater since information is available to unauthorized users.
- Operating efficiency is enhanced since anyone can print any report at any time.
- Operating procedures are more effective since information is easily available.
- User friendliness and flexibility is facilitated since there is a smooth flow of information among users.

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Information in all its forms needs to be protected from unauthorized access. Unrestricted access to the report option results in an exposure. Efficiency and effectiveness are not relevant factors in this situation. Greater control over reports will not be accomplished since reports need not be in a printed form only. Information could be transmitted outside as electronic files, because print options allow for printing in an electronic form as well.

---

**QUESTION 691**
Sign-on procedures include the creation of a unique user ID and password. However, an IS auditor discovers that in many cases the username and password are the same. The BEST control to mitigate this risk is to:
- Change the company's security policy.
- Educate users about the risk of weak passwords.

- Build in validations to prevent this during user creation and password change.
- Require a periodic review of matching user ID and passwords for detection and correction.

**Correct Answer:** C
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The compromise of the password is the highest risk. The best control is a preventive control through validation at the time the password is created or changed. Changing the company's security policy and educating users about the risks of weak passwords only provides information to users, but does little to enforce this control. Requiring a periodic review of matching user ID and passwords for detection and ensuring correction is a detective control.

---

**QUESTION 692**
The PRIMARY objective of a logical access control review is to:
- Review access controls provided through software.
- Ensure access is granted per the organization's authorities.
- Walk through and assess the access provided in the IT environment.
- Provide assurance that computer hardware is adequately protected against abuse.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The scope of a logical access control review is primarily to determine whether or not access is granted per the organization's authorizations. Choices A and C relate to procedures of a logical access control review, rather than objectives. Choice D is relevant to a physical access control review.

---

**QUESTION 693**
Naming conventions for system resources are important for access control because they:
- Ensure that resource names are not ambiguous.
- Reduce the number of rules required to adequately protect resources.
- Ensure that user access to resources is clearly and uniquely identified.
- Ensure that internationally recognized names are used to protect resources.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Naming conventions for system resources are important for the efficient administration of security controls. The conventions can be structured, so resources beginning with the same high-level qualifier can be governed by one or more generic rules. This reduces the number of rules required to adequately protect resources, which in turn facilitates security administration and maintenance efforts. Reducing the number of rules required to protect resources allows for the grouping of resources and files by application, which makes it easier to provide access. Ensuring that resource names are not ambiguous cannot be achieved through the use of naming conventions. Ensuring the clear and unique identification of user access to resources is handled by access control rules, not naming conventions. Internationally recognized names are not required to control access to resources. Naming conventions tend to be based on how each organization wants to identify its resources.

---

**QUESTION 694**
Which of the following exposures could be caused by a line grabbing technique?
- Unauthorized data access
- Excessive CPU cycle usage
- Lockout of terminal polling
- Multiplexor control dysfunction

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**

Line grabbing will enable eavesdropping, thus allowing unauthorized data access; it will not necessarily cause multiplexor dysfunction, excessive CPU usage, or lockout of terminal polling.

---

**QUESTION 695**
Electromagnetic emissions from a terminal represent an exposure because they:
- Affect noise pollution.
- Disrupt processor functions.
- Produce dangerous levels of electric current.
- Can be detected and displayed.

**Correct Answer:** D
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Emissions can be detected by sophisticated equipment and displayed, thus giving unauthorized persons access to data. They should not cause disruption of CPUs or affect noise pollution.

---

**QUESTION 696**
Security administration procedures require read-only access to:
- Access control tables.
- Security log files.
- Logging options.
- User profiles.

**Correct Answer:** B
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Security administration procedures require read-only access to security log files to ensure that, once generated, the logs are not modified. Logs provide evidence and track suspicious transactions and activities. Security administration procedures require write access to access control tables to manage and update the privileges according to authorized business requirements. Logging options require write access to allow the administrator to update how transactions and user activities are monitored, captured, stored, processed, and reported.

---

**QUESTION 697**
With the help of a security officer, granting access to data is the responsibility of:
- Data owners.
- Programmers.
- System analysts.
- Librarians.

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Data owners are responsible for the use of data. Written authorization for users to gain access to computerized information should be provided by the data owners. Security administration, with the owners' approval, sets up access rules stipulating which users or groups of users are authorized to access data or files and the level of authorized access (e.g., read or update).

---

**QUESTION 698**
The FIRST step in data classification is to:
- Establish ownership.
- Perform a criticality analysis.
- Define access rules.
- Create a data dictionary.

**Correct Answer:** A

**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Data classification is necessary to define access rules based on a need-to-do and need-to-know basis. The data owner is responsible for defining the access rules; therefore, establishing ownership is the first step in data classification. The other choices are incorrect. A criticality analysis is required for the protection of data, which takes input from data classification. Access definition is complete after data classification, and input for a data dictionary is prepared from the data classification process.

---

**QUESTION 699**
Which of the following provides the framework for designing and developing logical access controls?

- Information systems security policy
- Access control lists
- Password management
- System configuration files

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
The information systems security policy developed and approved by an organization's top management is the basis upon which logical access control is designed and developed. Access control lists, password management, and systems configuration files are tools for implementing the access controls.

---

**QUESTION 700**
A hacker could obtain passwords without the use of computer tools or programs through the technique of:

- Social engineering.
- Sniffers.
- Back doors.
- Trojan horses.

**Correct Answer:** A
**Section:** PROTECTION OF INFORMATION ASSETS
**Explanation:**
Social engineering is based on the divulgence of private information through dialogues and interviews.