QUESTION 901
An organization with extremely high security requirements is evaluating the effectiveness of biometric systems. Which of the following performance indicators is MOST important?
- False-acceptance rate (FAR)
- Equal-error rate (EER)
- False-rejection rate (FRR)
- False-identification rate (FIR)

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
FAR is the frequency of accepting an unauthorized person as authorized, thereby granting access when it should be denied. In an organization with high security requirements, user annoyance with a higher FRR is less important, since it is better to deny access to an authorized individual than to grant access to an unauthorized individual. EER is the point where the FAR equals the FRR; therefore, it does not minimize the FAR. FIR is the probability that an authorized person is identified but is assigned a false ID.

QUESTION 902
The MOST effective control for addressing the risk of piggybacking is:
- a single entry point with a receptionist.
- the use of smart cards.
- a biometric door lock.
- a deadman door.

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding area. This reduces the risk of an unauthorized person following an authorized person through a secured entry (piggybacking). The other choices are all physical controls over entry to a secure area but do not specifically address the risk of piggybacking.

QUESTION 903
The BEST overall quantitative measure of the performance of biometric control devices is:
- false-rejection rate.
- false-acceptance rate.
- equal-error rate.
- estimated-error rate.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
A low equal-error rate (EER) is a combination of a low false-rejection rate and a low false-acceptance rate. EER, expressed as a percentage, is a measure of the number of times that the false-rejection and false-acceptance rates are equal. A low EER is the measure of the more effective biometrics control device. Low false-rejection rates or low false-acceptance rates alone do not measure the efficiency of the device. Estimated-error rate is nonexistent and therefore irrelevant.

QUESTION 904
Which of the following is the MOST effective control over visitor access to a data center?
- Visitors are escorted.
- Visitor badges are required.
- Visitors sign in.
- Visitors are spot-checked by operators.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Escorting visitors will provide the best assurance that visitors have permission to access the data processing facility. Choices B and C are not reliable controls. Choice D is incorrect because visitors should be accompanied at all times while they are on the premises, not only when they are in the data processing facility.

QUESTION 905
The use of residual biometric information to gain unauthorized access is an example of which of the following attacks?

- Replay
- Brute force
- Cryptographic
- Mimic

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Residual biometric characteristics, such as fingerprints left on a biometric capture device, may be reused by an attacker to gain unauthorized access. A brute force attack involves feeding the biometric capture device numerous different biometric samples. A cryptographic attack targets the algorithm or the encrypted data; in a mimic attack, the attacker reproduces characteristics similar to those of the enrolled user, such as forging a signature or imitating a voice.

QUESTION 906
A firm is considering using biometric fingerprint identification on all PCs that access critical data. This requires:

- that a registration process is executed for all accredited PC users.
- the full elimination of the risk of a false acceptance.
- the usage of the fingerprint reader be accessed by a separate password.
- assurance that it will be impossible to gain unauthorized access to critical data.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The fingerprints of accredited users need to be read, identified, and recorded, i.e., registered, before a user may operate the system from the screened PCs. Choice B is incorrect, as the false-acceptance risk of a biometric device may be optimized, but will never be zero because this would imply an unacceptably high risk of false rejection. Choice C is incorrect, as the fingerprint device reads the token (the user's fingerprint) and does not need to be protected in itself by a password. Choice D is incorrect because the usage of biometric protection on PCs does not guarantee that other potential security weaknesses in the system may not be exploited to access protected data.

QUESTION 907
Which of the following biometrics has the highest reliability and lowest false-acceptance rate (FAR)?

- Palm scan
- Face recognition
- Retina scan
- Hand geometry

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Retina scan uses optical technology to map the capillary pattern of an eye's retina. This is highly reliable and has the lowest false-acceptance rate (FAR) among the current biometric methods. Use of palm scanning entails placing a hand on a scanner where a palm's physical characteristics are captured. Hand

geometry, one of the oldest techniques, measures the physical characteristics of the user's hands and fingers from a three-dimensional perspective. The palm and hand biometric techniques lack uniqueness in the geometry data. In face biometrics, a reader analyzes the images captured for general facial characteristics. Though considered a natural and friendly biometric, the main disadvantage of face recognition is the lack of uniqueness, which means that people looking alike can fool the device.

QUESTION 908
The MOST likely explanation for a successful social engineering attack is:
- that computers make logic errors.
- that people make judgment errors.
- the computer knowledge of the attackers.
- the technological sophistication of the attack method.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Humans make errors in judging others; they may trust someone when, in fact, the person is untrustworthy. Driven by logic, computers make the same error every time they execute the erroneous logic; however, this is not the basic argument in designing a social engineering attack. Generally, social engineering attacks do not require technological expertise; often, the attacker is not proficient in information technology or systems. Social engineering attacks are human-based and generally do not involve complicated technology.

QUESTION 909
The purpose of a deadman door controlling access to a computer facility is primarily to:
- prevent piggybacking.
- prevent toxic gases from entering the data center.
- starve a fire of oxygen.
- prevent an excessively rapid entry to, or exit from, the facility.

Correct Answer: A
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The purpose of a deadman door controlling access to a computer facility is primarily intended to prevent piggybacking. Choices B and C could be accomplished with a single self-closing door. Choice D is invalid, as a rapid exit may be necessary in some circumstances, e.g., a fire.

QUESTION 910
Which of the following is the MOST reliable form of single-factor personal identification?
- Smart card
- Password
- Photo identification
- Iris scan

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Since no two irises are alike, identification and verification can be done with confidence. There is no guarantee that a smart card is being used by the correct person since it can be shared, stolen, or lost and found. Passwords can be shared and, if written down, carry the risk of discovery. Photo IDs can be forged or falsified.

QUESTION 911
A data center has a badge-entry system. Which of the following is MOST important to protect the computing assets in the center?
- Badge readers are installed in locations where tampering would be noticed.

- The computer that controls the badge system is backed up frequently.
- A process for promptly deactivating lost or stolen badges exists.
- All badge entry attempts are logged.

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Tampering with a badge reader cannot open the door, so this is irrelevant. Logging the entry attempts may be of limited value. The biggest risk is from unauthorized individuals who can enter the data center, whether they are employees or not. Thus, a process of deactivating lost or stolen badges is important. The configuration of the system does not change frequently; therefore, frequent backup is not necessary.

QUESTION 912
Which of the following physical access controls effectively reduces the risk of piggybacking?
- Biometric door locks
- Combination door locks
- Deadman doors
- Bolting door locks

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Deadman doors use a pair of doors. For the second door to operate, the first entry door must close and lock with only one person permitted in the holding area. This effectively reduces the risk of piggybacking. An individual's unique body features such as voice, retina, fingerprint, or signature activate biometric door locks; however, they do not prevent or reduce the risk of piggybacking. Combination door locks, also known as cipher locks, use a numeric keypad or dial

QUESTION 913
The MOST effective biometric control system is the one:
- which has the highest equal-error rate (EER).
- which has the lowest EER.
- for which the false-rejection rate (FRR) is equal to the false-acceptance rate (FAR).
- for which the FRR is equal to the failure-to-enroll rate (FER).

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The equal-error rate (EER) of a biometric system denotes the percent at which the false-acceptance rate (FAR) is equal to the false-rejection rate (FRR). The biometric that has the lowest EER is the most effective. The biometric that has the highest EER is the most ineffective. For any biometric, there will be a measure at which the FRR will be equal to the FAR. This is the EER. FER is an aggregate measure of FRR.

QUESTION 914
Which of the following is the BEST way to satisfy a two-factor user authentication?
- A smart card requiring the user's PIN
- User ID along with password
- Iris scanning plus fingerprint scanning
- A magnetic card requiring the user's PIN

Correct Answer: A
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). An ID and password, what the user knows, is a single-factor user authentication. Choice C is not a two-factor user authentication because it is only biometric. Choice D is similar to choice A, but the magnetic card may be copied; therefore, choice A is the best way to satisfy a two-factor user authentication.

QUESTION 915

What should an organization do before providing an external agency physical access to its information processing facilities (IPFs)?

- The processes of the external agency should be subjected to an IS audit by an independent agency.
- Employees of the external agency should be trained on the security procedures of the organization.
- Any access by an external agency should be limited to the demilitarized zone (DMZ).
- The organization should conduct a risk assessment and design and implement appropriate controls.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Physical access of information processing facilities (IPFs) by an external agency introduces additional threats into an organization. Therefore, a risk assessment should be conducted and controls designed accordingly. The processes of the external agency are not of concern here. It is the agency's interaction with the organization that needs to be protected. Auditing their processes would not be relevant in this scenario. Training the employees of the external agency may be one control procedure but could be performed after access has been granted. Sometimes an external agency may require access to the processing facilities beyond the demilitarized zone (DMZ). For example, an agency that undertakes maintenance of servers may require access to the main server room. Restricting access within the DMZ will not serve the purpose.

QUESTION 916

An IS auditor is reviewing the physical security measures of an organization. Regarding the access card system, the IS auditor should be MOST concerned that:

- nonpersonalized access cards are given to the cleaning staff, who use a sign-in sheet but show no proof of identity.
- access cards are not labeled with the organization's name and address to facilitate easy return of a lost card.
- card issuance and rights administration for the cards are done by different departments, causing unnecessary lead time for new cards.
- the computer system used for programming the cards can only be replaced after three weeks in the event of a system failure.

Correct Answer: A

Section: PROTECTION OF INFORMATION ASSETS

Explanation:

Physical security is meant to control who is entering a secured area, so identification of all individuals is of utmost importance. It is not adequate to trust unknown external people by allowing them to write down their alleged name without proof, e.g., identity card, driver's license. Choice B is not a concern because if the name and address of the organization were written on the card, a malicious finder could use the card to enter the organization's premises. Separating card issuance from technical rights management is a method to ensure a proper segregation of duties so that no single person can produce a functioning card for a restricted area within the organization's premises. Choices B and C are good practices, not concerns. Choice D may be a concern, but not as important since a system failure of the card programming device would normally not mean that the readers do not function anymore. It simply means that no new cards can be issued, so this option is minor compared to the threat of improper identification.

QUESTION 917
Which of the following is the BEST way to handle obsolete magnetic tapes before disposing of them?
- Overwriting the tapes
- Initializing the tape labels
- Degaussing the tapes
- Erasing the tapes

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The best way to handle obsolete magnetic tapes is to degauss them. This action leaves a very low residue of magnetic induction, essentially erasing the data from the tapes. Overwriting or erasing the tapes may cause magnetic errors but would not remove the data completely. Initializing the tape labels would not remove the data that follows the label.

QUESTION 918
Which of the following is the MOST important objective of data protection?
- identifying persons who need access to information
- Ensuring the integrity of information
- Denying or authorizing access to the IS system
- Monitoring logical accesses

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Maintaining data integrity is the most important objective of data security. This is a necessity if an organization is to continue as a viable and successful enterprise. The other choices are important techniques for achieving the objective of data integrity.

QUESTION 919
Which of the following aspects of symmetric key encryption influenced the development of asymmetric encryption?
- Processing power
- Volume of data
- Key distribution
- Complexity of the algorithm

Correct Answer: C
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Symmetric key encryption requires that the keys be distributed. The larger the user group, the more challenging the key distribution. Symmetric key cryptosystems are generally less complicated and, therefore, use less processing power than asymmetric techniques, thus making it ideal for encrypting a large volume of data. The major disadvantage is the need to get the keys into the hands of those with whom you want to exchange data, particularly in e-commerce environments, where customers are unknown, untrusted entities.

QUESTION 920
A hard disk containing confidential data was damaged beyond repair. What should be done to the hard disk to prevent access to the data residing on it?
- Rewrite the hard disk with random Os and Is.
- Low-level format the hard disk.
- Demagnetize the hard disk.
- Physically destroy the hard disk.

Correct Answer: D

Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Physically destroying the hard disk is the most economical and practical way to ensure that the data cannot be recovered. Rewriting data and low-level formatting are impractical because the hard disk is damaged. Demagnetizing is an inefficient procedure, as it requires specialized and expensive equipment to be fully effective.

QUESTION 921
Which of the following is the MOST robust method for disposing of magnetic media that contains confidential information?

- Degaussing
- Defragmenting
- Erasing
- Destroying

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Destroying magnetic media is the only way to assure that confidential information cannot be recovered. Degaussing or demagnetizing is not sufficient to fully erase information from magnetic media. The purpose of defragmentation is to eliminate fragmentation in file systems and does not remove information. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.

QUESTION 922
Which of the following would MOST effectively control the usage of universal storage bus (USB) storage devices?

- Policies that require instant dismissal if such devices are found
- Software for tracking and managing USB storage devices
- Administratively disabling the USB port
- Searching personnel for USB storage devices at the facility's entrance

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Software for centralized tracking and monitoring would allow a USB usage policy to be applied to each user based on changing business requirements, and would provide for monitoring and reporting exceptions to management. A policy requiring dismissal may result in increased employee attrition, and business requirements would not be properly addressed. Disabling ports would be complex to manage and might not allow for new business needs. Searching personnel for USB storage devices at the entrance to a facility is not a practical solution since these devices are small and could be easily hidden.

QUESTION 923
An organization is disposing of a number of laptop computers. Which of the following data destruction methods would be the MOST effective?

- Run a low-level data wipe utility on all hard drives
- Erase all data file directories
- Format all hard drives
- Physical destruction of the hard drive

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
The most effective method is physical destruction. Running a low-level data wipe utility may leave some

residual data that could be recovered; erasing data directories and formatting hard drives are easily reversible, exposing all data on the drive to unauthorized individuals.

QUESTION 924
To ensure authentication, confidentiality, and integrity of a message, the sender should:
- Encrypt the hash of the message with the sender's public key and then encrypt the message with the receiver's private key.
- Encrypt the hash of the message with the sender's private key and then encrypt the message with the receiver's public key.
- Encrypt the hash of the message with the sender's public key and then encrypt the message with the receiver's public key.
- Encrypt the hash of the message with the sender's private key and then encrypt the message with the receiver's private key.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Obtaining the hash of the message ensures integrity; signing the hash of the message with the sender's private key ensures the authenticity of the origin, and encrypting the resulting message with the receiver's public key ensures confidentiality. The other choices are incorrect.

QUESTION 925
Which of the following would be the MOST significant audit finding when reviewing a point-of-sale (POS) system?
- Invoices recorded on the POS system are manually entered into an accounting application
- An optical scanner is not used to read bar codes for the generation of sales invoices
- Frequent power outages occur, resulting in the manual preparation of invoices
- Customer credit card information is stored unencrypted on the local POS system

Correct Answer: D
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
It is important for the IS auditor to determine if any credit card information is stored on the local point-of-sale (POS) system. Any such information, if stored, should be encrypted or protected by other means to avoid the possibility of unauthorized disclosure. Manually inputting sale invoices into the accounting application is an operational issue. The nonavailability of optical scanners to read bar codes of the products and power outages are also operational issues but do not pose the same level of risk as unencrypted credit card information.

QUESTION 926
When reviewing the procedures for the disposal of computers, which of the following should be the GREATEST concern for the IS auditor?
- Hard disks are overwritten several times at the sector level, but are not reformatted before leaving the organization.
- All files and folders on hard disks are separately deleted, and the hard disks are formatted before leaving the organization.
- Hard disks are rendered unreadable by hole-punching through the platters at specific positions before leaving the organization.
- The transport of hard disks is escorted by internal security staff to a nearby metal recycling company, where the hard disks are registered and then shredded.

Correct Answer: B
Section: PROTECTION OF INFORMATION ASSETS
Explanation:
Deleting and formatting does not completely erase the data but only marks the sectors that contained files as being free. There are tools available over the Internet that allow one to reconstruct most of a

hard disk's contents. Overwriting a hard disk at the sector level would completely erase data, directories, indices, and master file tables. While hole-punching does not delete file contents, the hard disk cannot be used anymore, especially when head parking zones and track zero information are impacted.

QUESTION 927
At a hospital, medical personnel carry handheld computers that contain patient health data. These handheld computers are synchronized with PCs that transfer data from a hospital database. Which of the following would be of the most importance?

- The handheld computers are properly protected to prevent loss of data confidentiality, in case of theft or loss.
- The employee who deletes temporary files from the local PC, after usage, is authorized to maintain PCs.
- Timely synchronization is ensured by policies and procedures.
- The usage of the handheld computers is allowed by the hospital policy.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Data confidentiality is a major requirement of privacy regulations. Choices B, C, and D relate to internal security requirements, which are secondary compared to compliance with data privacy laws.

QUESTION 928
Which of the following would BEST support 24/7 availability?

- Daily backup
- Offsite storage
- Mirroring
- Periodic testing

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Mirroring of critical elements is a tool that facilitates immediate recoverability. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately. Offsite storage and periodic testing of systems do not by themselves support continuous availability.

QUESTION 929
The PRIMARY purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

- Achieve performance improvement.
- Provide user authentication.
- Ensure availability of data.
- Ensure the confidentiality of data.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
RAID level 1 provides disk mirroring. Data written to one disk are also written to another disk. Users in the network access data in the first disk; if disk one fails, the second disk takes over. This redundancy ensures the availability of data. RAID level 1 does not improve performance, has no relevance to authentication, and does nothing to provide for data confidentiality.

QUESTION 930
Which of the following is the MOST important criterion when selecting a location for an offsite storage facility for IS backup files? The offsite facility must be:

- Physically separated from the data center and not subject to the same risks.
- Given the same level of protection as that of the computer data center.

- Outsourced to a reliable third party.
- Equipped with surveillance capabilities.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
It is important that there be an offsite storage location for IS files and that it be in a location not subject to the same risks as the primary data center. The other choices are all issues that must be considered when establishing the offsite location, but they are not as critical as the location selection.

QUESTION 931
If a database is restored using before-image dumps, where should the process begin following an interruption?

- Before the last transaction
- After the last transaction
- As the first transaction after the latest checkpoint
- As the last transaction before the latest checkpoint

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken. The last transaction will not have updated the database and must be reprocessed. Program checkpoints are irrelevant in this situation.

QUESTION 932
In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

- Maintaining system software parameters
- Ensuring periodic dumps of transaction logs
- Ensuring grandfather-father-son file backups
- Maintaining important data at an offsite location

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historical data. The volume of activity usually associated with an online system makes other more traditional methods of backup impractical.

QUESTION 933
As updates to an online order entry system are processed, the updates are recorded on a transaction tape and a hard copy transaction log. At the end of the day, the order entry files are backed up on tape. During the backup procedure, a drive malfunctions and the order entry files are lost. Which of the following is necessary to restore these files?

- The previous day's backup file and the current transaction tape
- The previous day's transaction file and the current transaction tape
- The current transaction tape and the current hard copy transaction log
- The current hard copy transaction log and the previous day's transaction file

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The previous day's backup file will be the most current historical backup of activity in the system. The current day's transaction file will contain all of the day's activity. Therefore, the combination of these two files will enable full recovery up to the point of interruption.

QUESTION 934
An offsite information processing facility:
- Should have the same amount of physical access restrictions as the primary processing site.
- Should be easily identified from the outside so that, in the event of an emergency, it can be easily found.
- Should be located in proximity to the originating site, so it can quickly be made operational.
- Need not have the same level of environmental monitoring as the originating site.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
An offsite information processing facility should have the same amount of physical control as the originating site. It should not be easily identified from the outside to prevent intentional sabotage. The offsite facility should not be subject to the same natural disaster that could affect the originating site and thus should not be located in proximity to the original site. The offsite facility should possess the same level of environmental monitoring and control as the originating site.

QUESTION 935
An IS auditor performing a review of the backup processing facilities should be MOST concerned that:
- Adequate fire insurance exists.
- Regular hardware maintenance is performed.
- Offsite storage of transaction and master files exists.
- Backup processing facilities are fully tested.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Adequate fire insurance and fully tested backup processing facilities are important elements for recovery, but without the offsite storage of transaction and master files, it is generally impossible to recover. Regular hardware maintenance does not relate to recovery.

QUESTION 936
Which of the following procedures would BEST determine whether adequate recovery/restart procedures exist?
- Reviewing program code
- Reviewing operations documentation
- Turning off the UPS, then the power
- Reviewing program documentation

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Operations documentation should contain recovery/restart procedures, so operations can return to normal processing in a timely manner. Turning off the uninterruptible power supply (UPS) and then turning off the power might create a situation for recovery and restart, but the negative effect on operations would prove this method to be undesirable. The review of program code and documentation generally does not provide evidence regarding recovery/restart procedures.

QUESTION 937
Which of the following findings should an IS auditor be MOST concerned about when performing an audit of backup and recovery and the offsite storage vault?
- There are three individuals with a key to enter the area.
- Paper documents are also stored in the offsite vault.
- Data files that are stored in the vault are synchronized.
- The offsite vault is located in a separate facility.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Choice A is incorrect because more than one person would typically need to have a key to the vault to ensure that individuals responsible for the offsite vault can take vacations and rotate duties. Choice B is not correct because an IS auditor would not be concerned with whether paper documents are stored in the offsite vault. In fact, paper documents, such as procedural documents and a copy of the contingency plan, would most likely be stored in the offsite vault, and the location of the vault is important, but not as important as the files being synchronized.

QUESTION 938
Online banking transactions are being posted to the database when processing suddenly comes to a halt. The integrity of the transaction processing is BEST ensured by:

- Database integrity checks.
- Validation checks.
- Input controls.
- Database commits and rollbacks.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Database commits ensure the data are saved to disk, while the transaction processing is underway or complete. Rollback ensures that the already completed processing is reversed back, and the data already processed are not saved to the disk in the event of the failure of the completion of the transaction processing. All other options do not ensure integrity while processing is underway.

QUESTION 939
To provide protection for media backup stored at an offsite location, the storage site should be:

- Located on a different floor of the building.
- Easily accessible by everyone.
- Clearly labeled for emergency access.
- Protected from unauthorized access.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The offsite storage site should always be protected against unauthorized access and have at least the same security requirements as the primary site. Choice A is incorrect because if the backup is in the same building, it may suffer the same event and may be inaccessible. Choices B and C represent access risks.

QUESTION 940
Which of the following ensures the availability of transactions in the event of a disaster?

- Send tapes hourly containing transactions offsite.
- Send tapes daily containing transactions offsite.
- Capture transactions to multiple storage devices.
- Transmit transactions offsite in real time.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility. Choices A and B are not in real time and, therefore, would not include all the transactions. Choice C does not ensure availability at an offsite location.

QUESTION 941
IS management has decided to install a level 1 Redundant Array of Inexpensive Disks (RAID) system in all servers to compensate for the elimination of offsite backups. The IS auditor should recommend:
- Upgrading to a level 5 RAID.
- Increasing the frequency of onsite backups.
- Reinstating the offsite backups.
- Establishing a cold site in a secure location.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups, more frequent onsite backups, or even setting up a cold site. Choices A, B, and D do not compensate for the lack of offsite backup.

QUESTION 942
In which of the following situations is it MOST appropriate to implement data mirroring as the recovery strategy?
- Disaster tolerance is high.
- Recovery time objective is high.
- Recovery point objective is low.
- Recovery point objective is high.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A recovery point objective (RPO) indicates the latest point in time at which it is acceptable to recover the data. If the RPO is low, data mirroring should be implemented as the data recovery strategy. The recovery time objective (RTO) is an indicator of disaster tolerance. The lower the RTO, the lower the disaster tolerance.

QUESTION 943
Network Data Management Protocol (NDMP) technology should be used for backup if:
- A network attached storage (NAS) appliance is required.
- The use of TCP/IP must be avoided.
- File permissions that cannot be handled by legacy backup systems must be backed up.
- Backup consistency over several related data volumes must be ensured.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
NDMP is particularly useful for NAS environments where it is challenging to install backup software agents. NDMP optimizes backup performance and addresses the challenges of backing up NAS devices.

QUESTION 944
An organization currently using tape backups takes one full backup weekly and incremental backups daily. They recently augmented their tape backup procedures with a backup-to-disk solution. This is appropriate because:
- Fast synthetic backups for offsite storage are supported.
- Backup to disk is always significantly faster than backup to tape.
- Tape libraries are no longer needed.
- Data storage on disks is more reliable than on tapes.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:

Disk-to-disk (D2D) backup is not a direct replacement for tape but enhances the backup architecture. It enables fast synthetic backups, which can improve recovery performance.

QUESTION 945
Which of the following should be the MOST important criterion in evaluating a backup solution for sensitive data that must be retained for a long period due to regulatory requirements?

- Full backup window
- Media costs
- Restore window
- Media reliability

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Media reliability is crucial for ensuring the organization's ability to recover data, especially for compliance with regulatory requirements. Other factors, while important, should not take precedence over media reliability.

QUESTION 946
In the event of a data center disaster, which of the following would be the MOST appropriate strategy to enable a complete recovery of a critical database?

- Daily data backup to tape and storage at a remote site
- Real-time replication to a remote site
- Hard disk mirroring to a local server
- Real-time data backup to the local storage area network (SAN)

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Real-time replication to a remote site ensures that data is continuously updated, minimizing data loss during a disaster. Other options may not provide the same level of protection against data loss.

QUESTION 947
Which of the following backup techniques is the MOST appropriate when an organization requires extremely granular data restore points, as defined in the recovery point objective (RPO)?

- Virtual tape libraries
- Disk-based snapshots
- Continuous data backup
- Disk-to-tape backup

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Continuous data backup allows for real-time data protection, ensuring extremely granular restore points that align with a low RPO.

QUESTION 948
What is the BEST backup strategy for a large database with data supporting online sales?

- Weekly full backup with daily incremental backup
- Daily full backup
- Clustered servers
- Mirrored hard disks

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:

A weekly full backup combined with daily incremental backups balances recovery capabilities and minimizes daily backup times, making it practical for a large database.

QUESTION 949
During an audit, an IS auditor notes that an organization's business continuity plan (BCP) does not adequately address information confidentiality during a recovery process. The IS auditor should recommend that the plan be modified to include:

- The level of information security required when business recovery procedures are invoked.
- Information security roles and responsibilities in the crisis management structure.
- Information security resource requirements.
- Change management procedures for information security that could affect business continuity arrangements.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
It's essential for the BCP to specify the level of information security needed during recovery, especially regarding access to confidential data.

QUESTION 950
Which of the following is the GREATEST risk when storage growth in a critical file server is not managed properly?

- Backup time would steadily increase
- Backup operational cost would significantly increase
- Storage operational cost would significantly increase
- Server recovery work may not meet the recovery time objective (RTO)

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
If the growth of data is unmanaged, the time required to recover the server may exceed the RTO, leading to significant operational issues.

QUESTION 951
Which of the following is the MOST important consideration when defining recovery point objectives (RPOs)?

- Minimum operating requirements
- Acceptable data loss
- Mean time between failures
- Acceptable time for recovery

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The primary purpose of an RPO is to define the maximum acceptable data loss that the organization can tolerate in the event of a disruption. This is critical for determining how frequently data should be backed up or replicated to ensure recovery aligns with the organization’s data loss tolerance. While other factors like minimum operating requirements, mean time between failures, and acceptable time for recovery are relevant to continuity planning, they do not directly address the purpose of an RPO, which focuses specifically on setting acceptable data loss limits.

QUESTION 952
A structured walk-through test of a disaster recovery plan involves:

- Representatives from each of the functional areas coming together to go over the plan.

- All employees who participate in the day-to-day operations coming together to practice executing the plan.
- Moving the systems to the alternate processing site and performing processing operations.
- Distributing copies of the plan to the various functional areas for review.

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A structured walk-through test of a disaster recovery plan involves **all employees who participate in the day-to-day operations coming together to practice executing the plan**. This exercise helps ensure that everyone understands their roles and responsibilities, allowing for a practical review of the plan's effectiveness and identifying any potential issues. Unlike simple plan reviews or system relocations, this test actively engages key staff members in simulating a disaster response.

QUESTION 953
In a contract with a hot, warm, or cold site, contractual provisions should cover which of the following considerations?

- Physical security measures
- Total number of subscribers
- Number of subscribers permitted to use a site at one time
- References by other users

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
When contracting for a hot, warm, or cold site, it is essential to include provisions that specify **the number of subscribers permitted to use the site at one time**. This ensures that the site will be available to meet the organization’s recovery needs during an emergency by preventing oversubscription and resource contention. Although factors like physical security, total subscriber numbers, and references by other users are also important, they do not directly address the critical need to control simultaneous usage, which could impact site availability during a disaster.

QUESTION 954
Which of the following is the GREATEST concern when an organization's backup facility is at a warm site?

- Timely availability of hardware
- Availability of heat, humidity, and air conditioning equipment
- Adequacy of electrical power connections
- Effectiveness of the telecommunications network

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The **greatest concern with a warm site** is the **timely availability of hardware**. Unlike a hot site, a warm site typically does not have all hardware immediately in place; some equipment may need to be acquired or transported in the event of a disaster. This could delay recovery operations. While factors such as environmental controls, power connections, and telecommunications are also important, they are generally more readily available or easily addressed compared to the potential delay in obtaining critical hardwar

---

QUESTION 955
Which of the following recovery strategies is MOST appropriate for a business having multiple offices within a region and a limited recovery budget?

- A hot site maintained by the business
- A commercial cold site
- A reciprocal arrangement between its offices
- A third-party hot site

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A **reciprocal arrangement between its offices** is the most suitable recovery strategy for a business with multiple regional offices and a limited budget. This arrangement allows each office to act as a backup for the others, leveraging existing resources without the need for additional expenditure on dedicated recovery facilities. This is a cost-effective solution compared to hot or cold sites, which involve additional costs, making it ideal for businesses with budget constraints.

QUESTION 956
The PRIMARY purpose of a business impact analysis (BIA) is to:

- Provide a plan for resuming operations after a disaster.
- Identify the events that could impact the continuity of an organization's operations.
- Publicize the commitment of the organization to physical and logical security.
- Provide the framework for an effective disaster recovery plan.

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The **primary purpose of a business impact analysis (BIA)** is to **identify the events that could impact the continuity of an organization's operations**. The BIA helps to assess potential risks, evaluate the effects of disruptions, and prioritize critical business functions for recovery planning. While a BIA supports the creation of a disaster recovery plan, its main focus is on understanding the risks and impacts on operations to inform strategic decision-making.

QUESTION 957
After implementation of a disaster recovery plan, pre-disaster and post-disaster operational costs for an organization will:

- Decrease.
- Not change (remain the same).
- Increase.
- Increase or decrease depending upon the nature of the business.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
After implementing a disaster recovery plan, **operational costs are likely to increase**. This is because maintaining a disaster recovery plan typically involves ongoing costs such as maintaining backup systems, acquiring additional resources (e.g., hardware, software, or off-site facilities), and training staff. While these costs help mitigate the impact of a disaster, they often result in higher operational expenses both before and after a disaster occurs.

QUESTION 958
Which of the following is the MOST reasonable option for recovering a noncritical system?

- Warm site
- Mobile site
- Hot site
- Cold site

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A **cold site** is the most reasonable option for recovering a noncritical system. Cold sites are typically less expensive and offer the basic infrastructure (such as space and power) needed to get systems up and running, but they do not have pre-configured equipment or systems in place. For noncritical systems, which do not require immediate or highly available recovery, a cold site provides a cost-effective solution without the need for more expensive options like hot or warm sites.

QUESTION 959
An organization having a number of offices across a wide geographical area has developed a disaster recovery plan. Using actual resources, which of the following is the MOST cost-effective test of the disaster recovery plan?

- Full operational test
- Preparedness test
- Paper test
- Regression test

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A **preparedness test** is the most cost-effective option for testing a disaster recovery plan using actual resources. This type of test typically involves practicing the execution of recovery procedures without fully implementing all systems or disrupting operations, making it less resource-intensive than a full operational test. A preparedness test allows the organization to assess its readiness and identify potential gaps in the recovery plan without incurring the high costs associated with more comprehensive tests, such as full operational or regression tests.

QUESTION 960
An organization's disaster recovery plan should address early recovery of:

- All information systems processes.
- All financial processing applications.
- Only those applications designated by the IS manager.
- Processing in priority order, as defined by business management.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The disaster recovery plan should focus on the **early recovery of processing in priority order, as defined by business management**. Business management typically determines which applications and systems are most critical to the organization's operations, and these should be restored first to minimize downtime and business impact. This approach ensures that recovery efforts align with the organization’s priorities and supports essential functions during the disaster recovery process.

QUESTION 961
An advantage of the use of hot sites as a backup alternative is that:

- The costs associated with hot sites are low.
- Hot sites can be used for an extended amount of time.
- Hot sites can be made ready for operation within a short period of time.
- They do not require that equipment and systems software be compatible with the primary site.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The main advantage of hot sites is that **they can be made ready for operation within a short period of time**. A hot site is fully equipped and ready to take over operations immediately or with minimal downtime in the event of a disaster, making it a critical resource for ensuring business continuity. While hot sites are expensive and require compatible systems, their primary benefit is the speed at which they can be activated to resume business operations.

QUESTION 962
Which of the following is a practice that should be incorporated into the plan for testing disaster recovery procedures?

- Invite client participation.
- Involve all technical staff.
- Rotate recovery managers.
- Install locally-stored backup.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Rotating recovery managers is a best practice to incorporate into the disaster recovery testing plan. This ensures that multiple managers are trained and prepared to lead recovery efforts, reducing dependency on any single individual. It also helps to evaluate how different managers handle disaster recovery procedures, ensuring a broader level of preparedness and flexibility in the event of a disaster. This practice supports the resilience and effectiveness of the organization's disaster recovery plan.

QUESTION 963
Disaster recovery planning (DRP) addresses the:

- Technological aspect of business continuity planning.
- Operational piece of business continuity planning.
- Functional aspect of business continuity planning.
- Overall coordination of business continuity planning.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Disaster recovery planning (DRP) primarily addresses the **technological aspect of business continuity planning**. DRP focuses on the recovery of IT infrastructure, systems, applications, and data after a disaster, ensuring that technology systems can be restored quickly to minimize disruption to business operations. While business continuity planning covers broader aspects, such as operations and overall coordination, DRP specifically targets the technological resources needed to resume business functions after a disaster.

QUESTION 964
An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

- The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
- The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting their attention.

- The plan has never been updated, tested, or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The IS auditor's report should recommend that:

- The deputy CEO be censured for their failure to approve the plan.
- A board of senior managers is set up to review the existing plan.
- The existing plan is approved and circulated to all key management and staff.
- A manager coordinates the creation of a new or revised plan within a defined time limit.

Correct Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The IS auditor should recommend that **a manager coordinates the creation of a new or revised plan within a defined time limit**. This recommendation addresses the gaps in the current disaster recovery plan, which has not been updated or formally tested. While the plan exists, its lack of approval, updates, and circulation means it cannot effectively serve its purpose. Appointing a manager to oversee the development and revision of a comprehensive disaster recovery plan with clear timelines ensures the plan is current, tested, and aligned with the organization's operational needs. This approach also fosters accountability and timely action.

QUESTION 965

An IS auditor conducting a review of disaster recovery planning (DRP) at a financial processing organization has discovered the following:

- The existing disaster recovery plan was compiled two years earlier by a systems analyst in the organization's IT department using transaction flow projections from the operations department.
- The plan was presented to the deputy CEO for approval and formal issue, but it is still awaiting his/her attention.
- The plan has never been updated, tested, or circulated to key management and staff, though interviews show that each would know what action to take for its area in the event of a disruptive incident.

The basis of an organization's disaster recovery plan is to reestablish live processing at an alternative site where a similar, but not identical, hardware configuration is already established. An IS auditor should:

- Take no action as the lack of a current plan is the only significant finding.
- Recommend that the hardware configuration at each site is identical.
- Perform a review to verify that the second configuration can support live processing.
- Report that the financial expenditure on the alternative site is wasted without an effective plan.

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The IS auditor should **perform a review to verify that the second configuration can support live processing**. Since the disaster recovery plan is based on a similar, but not identical, hardware configuration at the alternative site, it is crucial to ensure that the alternate hardware can handle the live processing requirements of the organization. This review would confirm that the site and its hardware are capable of supporting the business operations in the event of a disaster, ensuring that the recovery plan is both feasible and effective.

QUESTION 966

Disaster recovery planning (DRP) for a company's computer system usually focuses on:

- A. Operations turnover procedures
- B. Strategic long-range planning
- C. The probability that a disaster will occur

- D. Alternative procedures to process transactions

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
It is important that disaster recovery identifies alternative processes that can be put in place while the system is not available.

QUESTION 967
The MAIN purpose for periodically testing offsite facilities is to:

- A. Protect the integrity of the data in the database
- B. Eliminate the need to develop detailed contingency plans
- C. Ensure the continued compatibility of the contingency facilities
- D. Ensure that program and system documentation remains current

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities. Specific software tools are available to protect the ongoing integrity of the database. Contingency plans should not be eliminated and program and system documentation should be reviewed continuously for currency.

QUESTION 968
A large chain of shops with electronic funds transfer (EFT) at point-of-sale devices has a central communications processor for connecting to the banking network. Which of the following is the BEST disaster recovery plan for the communications processor?

- A. Offsite storage of daily backups
- B. Alternative standby processor onsite
- C. Installation of duplex communication links
- D. Alternative standby processor at another network node

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Having an alternative standby processor at another network node would be the best solution. The unavailability of the central communications processor would disrupt all access to the banking network, resulting in the disruption of operations for all the shops. This could be caused by failure of equipment, power, or communications. Offsite storage of backups would not help, since EFT tends to be an online process and offsite storage will not replace the dysfunctional processor. The provision of an alternate processor onsite would be fine if it were an equipment problem, but would not help in the case of a power outage. Installation of duplex communication links would be most appropriate if it were only the communication link that failed.

QUESTION 969
Facilitating telecommunications continuity by providing redundant combinations of local carrier T-1 lines, microwaves, and/or coaxial cables to access the local communication loop:

- A. Last-mile circuit protection
- B. Long-haul network diversity
- C. Diverse routing
- D. Alternative routing

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The method of providing telecommunication continuity through the use of many recovery facilities, providing redundant combinations of local carrier T-1s, microwave, and/or coaxial cable to access the

local communication loop in the event of a disaster, is called last-mile circuit protection. Providing diverse long-distance network availability utilizing T-1 circuits among major long-distance carriers is called long-haul network diversity. This ensures long-distance access should any one carrier experience a network failure. The method of routing traffic through split-cable facilities or duplicate-cable facilities is called diverse routing. Alternative routing is the method of routing information via an alternative medium, such as copper cable or fiber optics.

QUESTION 970

Which of the following represents the GREATEST risk created by a reciprocal agreement for disaster recovery made between two companies?

- A. Developments may result in hardware and software incompatibility
- B. Resources may not be available when needed
- C. The recovery plan cannot be tested
- D. The security infrastructures in each company may be different

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

If one organization updates its hardware and software configuration, it may mean that it is no longer compatible with the systems of the other party in the agreement. This may mean that each company is unable to use the facilities at the other company to recover their processing following a disaster. Resources being unavailable when needed are an intrinsic risk in any reciprocal agreement, but this is a contractual matter and is not the greatest risk. The plan can be tested by paper-based walkthroughs, and possibly by agreement between the companies. The difference in security infrastructures, while a risk, is not insurmountable.

QUESTION 971

Which of the following would BEST ensure continuity of a wide area network (WAN) across the organization?

- A. Built-in alternative routing
- B. Completing full system backup daily
- C. A repair contract with a service provider
- D. A duplicate machine alongside each server

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Alternative routing would ensure the network continues if a server is lost or if a link is severed, as message rerouting could be automatic. System backups won't provide immediate protection, and a repair contract is less effective than alternative routing. Standby servers will not provide continuity if a link is severed.

QUESTION 972

An IS auditor reviewing an organization's IS disaster recovery plan should verify that it is:

- A. Tested every six months
- B. Regularly reviewed and updated
- C. Approved by the chief executive officer (CEO)
- D. Communicated to every department head in the organization

Correct Answer: B

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The disaster recovery plan should be reviewed periodically to ensure its effectiveness. While testing is important, the frequency will depend on the organization. Senior management, such as the executive responsible for technology, may approve the plan, and it does not need to be communicated to all department heads if it is a technical document.

QUESTION 973
There are several methods of providing telecommunications continuity. The method of routing traffic through split cable or duplicate cable facilities is called:
- A. Alternative routing
- B. Diverse routing
- C. Long-haul network diversity
- D. Last-mile circuit protection

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Diverse routing routes traffic through split-cable or duplicate-cable facilities, ensuring continued communication in the event of a failure. Alternative routing involves using different networks or circuits, while long-haul network diversity ensures long-distance access. Last-mile circuit protection involves redundant access to local communication loops.

QUESTION 974
The responsibilities of a disaster recovery relocation team include:
- A. Obtaining, packaging, and shipping media and records to the recovery facilities, as well as establishing and overseeing an offsite storage schedule.
- B. Locating a recovery site, if one has not been predetermined, and coordinating the transport of company employees to the recovery site.
- C. Managing the relocation project and conducting a more detailed assessment of the damage to the facilities and equipment.
- D. Coordinating the process of moving from the hot site to a new location or to the restored original location.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The relocation team is responsible for coordinating the process of moving from a hot site to a new location or returning to the original site. Choices A, B, and C describe the responsibilities of other teams.

QUESTION 975
While reviewing the business continuity plan of an organization, an IS auditor observed that the organization's data and software files are backed up on a periodic basis. Which characteristic of an effective plan does this demonstrate?
- A. Deterrence
- B. Mitigation
- C. Recovery
- D. Response

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Mitigation refers to steps taken to reduce the effects of a disaster, such as regular backups. Deterrence involves preventive measures like firewalls, recovery is about restoration, and response refers to actions during a disaster.

QUESTION 976
Which of the following disaster recovery/continuity plan components provides the GREATEST assurance of recovery after a disaster?

- The alternate facility will be available until the original information processing facility is restored.
- User management is involved in the identification of critical systems and their associated critical recovery times.
- Copies of the plan are kept at the homes of key decision-making personnel.
- Feedback is provided to management assuring them that the business continuity plans are indeed workable and that the procedures are current.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The alternate facility should be made available until the original site is restored to provide the greatest assurance of recovery after a disaster. Without this assurance, the plan will not be successful. All other choices ensure prioritization or execution of the plan.

QUESTION 977

Which of the following must exist to ensure the viability of a duplicate information processing facility?

- The site is near the primary site to ensure quick and efficient recovery.
- The site contains the most advanced hardware available.
- The workload of the primary site is monitored to ensure adequate backup is available.
- The hardware is tested when it is installed to ensure it is working properly.

Correct Answer: C

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

Resource availability must be assured. The workload of the site must be monitored to ensure that availability for emergency backup use is not impaired. The site chosen should not be subject to the same natural disaster as the primary site. In addition, a reasonable compatibility of hardware/software must exist to serve as a basis for backup.

QUESTION 978

An offsite information processing facility with electrical wiring, air conditioning, and flooring, but no computer or communications equipment, is a:

- Cold site.
- Warm site.
- Dial-up site.
- Duplicate processing facility.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

A cold site is ready to receive equipment but does not offer any components at the site in advance of the need. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment to operate an information processing facility.

QUESTION 979

A disaster recovery plan for an organization should:

- Reduce the length of the recovery time and the cost of recovery.
- Increase the length of the recovery time and the cost of recovery.
- Reduce the duration of the recovery time and increase the cost of recovery.
- Affect neither the recovery time nor the cost of recovery.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

One of the objectives of a disaster recovery plan is to reduce the duration and cost of recovering from a disaster. The plan should reduce the time to return to normal operations and the cost that could result from a disaster.

QUESTION 980
A disaster recovery plan for an organization's financial system specifies that the recovery point objective (RPO) is no data loss and the recovery time objective (RTO) is 72 hours. Which of the following is the MOST cost-effective solution?

- A hot site that can be operational in eight hours with asynchronous backup of the transaction logs.
- Distributed database systems in multiple locations updated asynchronously.
- Synchronous updates of the data and standby active systems in a hot site.
- Synchronous remote copy of the data in a warm site that can be operational in 48 hours.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The synchronous copy of the storage achieves the RPO objective (no data loss) and the warm site operational in 48 hours meets the required RTO (72 hours). This solution is the most cost-effective compared to alternatives like hot sites with asynchronous backups or distributed database systems.

QUESTION 981
A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to automated teller machines (ATMs). Which of the following would be the BEST contingency plan for the communications processor?

- Reciprocal agreement with another organization
- Alternate processor in the same location
- Alternate processor at another network node
- Installation of duplex communication links

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The unavailability of the central communications processor would disrupt all access to the banking network. An alternate processor at another network node provides redundancy and is best suited to avoid a total loss in case of equipment, power, or communication failure. Reciprocal agreements raise privacy issues, and other options do not address environmental factors.

QUESTION 982
The cost of ongoing operations when a disaster recovery plan is in place, compared to not having a disaster recovery plan, will MOST likely:

- increase.
- decrease.
- remain the same.
- be unpredictable.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The cost of operations typically increases when a disaster recovery plan is implemented, due to the additional measures and resources required to maintain recovery capabilities during normal operations.

QUESTION 983
Which of the following tasks should be performed FIRST when preparing a disaster recovery plan?

- Develop a recovery strategy.
- Perform a business impact analysis.
- Map software systems, hardware and network components.

- Appoint recovery teams with defined personnel, roles and hierarchy.

Correct Answer: B

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The first step in preparing a disaster recovery plan is to perform a business impact analysis, which helps identify critical systems and their recovery needs. All other tasks follow this assessment.

QUESTION 984

Which of the following provides the BEST evidence of an organization's disaster recovery readiness?

- A disaster recovery plan
- Customer references for the alternate site provider
- Processes for maintaining the disaster recovery plan
- Results of tests and drills

Correct Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

The results of tests and drills provide the most reliable evidence of an organization's disaster recovery readiness, demonstrating that the plan and procedures are effective and up-to-date.

QUESTION 985

Which of the following is the BEST method for determining the criticality of each application system in the production environment?

- Interview the application programmers.
- Perform a gap analysis.
- Review the most recent application audits.
- Perform a business impact analysis.

Correct Answer: D

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

A business impact analysis (BIA) is the best method to assess the criticality of application systems by evaluating the impact of system loss on the business. Interviews with programmers and gap analysis may not provide a full assessment.

QUESTION 986

A hot site should be implemented as a recovery strategy when the:

- disaster tolerance is low.
- recovery point objective (RPO) is high.
- recovery time objective (RTO) is high.
- disaster tolerance is high.

Correct Answer: A

Section: BUSINESS CONTINUITY AND DISASTER RECOVERY

Explanation:

A hot site is used when disaster tolerance is low, meaning the organization cannot afford significant downtime. A hot site allows for rapid recovery, with minimal downtime.

QUESTION 987

An organization has implemented a disaster recovery plan. Which of the following steps should be carried out next?

- Obtain senior management sponsorship.
- Identify business needs.
- Conduct a paper test.
- Perform a system restore test.

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
After implementing a disaster recovery plan, the next step should be to conduct a paper test to verify that all elements of the plan are properly understood and in place before performing more extensive system tests.

QUESTION 988
When auditing a disaster recovery plan for a critical business area, an IS auditor finds that it does not cover all the systems. Which of the following is the MOST appropriate action for the IS auditor?

- Alert management and evaluate the impact of not covering all systems.
- Cancel the audit.
- Complete the audit of the systems covered by the existing disaster recovery plan.
- Postpone the audit until the systems are added to the disaster recovery plan.

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The IS auditor should alert management about the systems that are not covered in the disaster recovery plan and evaluate the impact of these gaps. Continuing with the audit will help assess the potential risks.

QUESTION 989
Which of the following should be of MOST concern to an IS auditor reviewing the BCP?

- The disaster levels are based on scopes of damaged functions, but not on duration.
- The difference between low-level disaster and software incidents is not clear.
- The overall BCP is documented, but detailed recovery steps are not specified.
- The responsibility for declaring a disaster is not identified.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The responsibility for declaring a disaster is critical, as the failure to invoke the recovery plan could result in significant delays or ineffective responses. This is the most pressing concern for the IS auditor.

QUESTION 990
Of the following alternatives, the FIRST approach to developing a disaster recovery strategy would be to assess whether:

- all threats can be completely removed.
- a cost-effective, built-in resilience can be implemented.
- the recovery time objective can be optimized.
- the cost of recovery can be minimized.

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The first step in developing a disaster recovery strategy is to assess whether built-in resilience (e.g., redundant systems, diverse routing) can be implemented. This helps ensure that critical systems are protected against disruptions.

QUESTION 991
An organization has a number of branches across a wide geographical area. To ensure that all aspects of the disaster recovery plan are evaluated in a cost-effective manner, an IS auditor should recommend the use of a:

- Data recovery test.
- Full operational test.
- Posttest.

- Preparedness test.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A preparedness test should be performed by each local office/area to test the adequacy of the preparedness of local operations in the event of a disaster. This test should be performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence of the plan's adequacy. A data recovery test is a partial test and will not ensure that all aspects are evaluated. A full operational test is not the most cost-effective test in light of the geographical dispersion of the branches, and a posttest is a phase of the test execution process.

QUESTION 992
If the recovery time objective (RTO) increases:

- **The disaster tolerance increases.**
- **The cost of recovery increases.**
- **A cold site cannot be used.**
- **The data backup frequency increases.**

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The longer the recovery time objective (RTO), the higher disaster tolerance and the lower the recovery cost. It cannot be concluded that a cold site is inappropriate or that the frequency of data backup would increase.

QUESTION 993
Due to changes in IT, the disaster recovery plan of a large organization has been changed. What is the PRIMARY risk if the new plan is not tested?

- **Catastrophic service interruption.**
- **High consumption of resources.**
- **Total cost of the recovery may not be minimized.**
- **Users and recovery teams may face severe difficulties when activating the plan.**

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Choices B, C, and D are all possible problems that might occur, and would cause difficulties and financial losses or waste of resources. However, if a new disaster recovery plan is not tested, the possibility of a catastrophic service interruption is the most critical of all risks.

QUESTION 994
When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

- **Annualized loss expectancy (ALE).**
- **Service delivery objective.**
- **Quantity of orphan data.**
- **Maximum tolerable outage.**

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The recovery time objective is determined based on the acceptable downtime in case of a disruption of operations, it indicates the maximum tolerable outage that an organization considers to be acceptable before a system or process must resume following a disaster. Choice A is incorrect, because the acceptable downtime would not be determined by the annualized loss expectancy (ALE). Choices B and C are relevant to business continuity, but they are not determined by acceptable downtime.

QUESTION 995
A lower recovery time objective (RTO) results in:
- Higher disaster tolerance.
- Higher cost.
- Wider interruption windows.
- More permissive data loss.

Correct Answer: B
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A recovery time objective (RTO) is based on the acceptable downtime in case of a disruption of operations. The lower the RTO, the higher the cost of recovery strategies. The lower the disaster tolerance, the narrower the interruption windows, and the lesser the permissive data loss.

QUESTION 996
Regarding a disaster recovery plan, the role of an IS auditor should include:
- Identifying critical applications.
- Determining the external service providers involved in a recovery test.
- Observing the tests of the disaster recovery plan.
- Determining the criteria for establishing a recovery time objective (RTO).

Correct Answer: C
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The IS auditor should be present when disaster recovery plans are tested, to ensure that the test meets the targets for restoration, and the recovery procedures are effective and efficient. As appropriate, the auditor should provide a report of the test results. All other choices are a responsibility of management.

QUESTION 997
During a disaster recovery test, an IS auditor observes that the performance of the disaster recovery site's server is slow. To find the root cause of this, the IS auditor should FIRST review the:
- **Event error log generated at the disaster recovery site.**
- **Disaster recovery test plan.**
- **Disaster recovery plan (DRP).**
- **Configurations and alignment of the primary and disaster recovery sites.**

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
Since the configuration of the system is the most probable cause, the IS auditor should review that first. If the issue cannot be clarified, the IS auditor should then review the event error log. The disaster recovery test plan and the disaster recovery plan (DRP) would not contain information about the system configuration.

QUESTION 998
An organization has a recovery time objective (RTO) equal to zero and a recovery point objective (RPO) close to 1 minute for a critical system. This implies that the system can tolerate:
- **A data loss of up to 1 minute, but the processing must be continuous.**
- **A 1-minute processing interruption but cannot tolerate any data loss.**
- **A processing interruption of 1 minute or more.**
- **Both a data loss and a processing interruption longer than 1 minute.**

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
The recovery time objective (RTO) measures an organization's tolerance for downtime and the recovery

point objective (RPO) measures how much data loss can be accepted. Choices B, C, and D are incorrect since they exceed the RTO limits set by the scenario.

QUESTION 999
Which of the following issues should be the GREATEST concern to the IS auditor when reviewing an IT disaster recovery test?

- Due to the limited test time window, only the most essential systems were tested. The other systems were tested separately during the rest of the year.
- During the test it was noticed that some of the backup systems were defective or not working, causing the test of these systems to fail.
- The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
- Every year, the same employees perform the test. The recovery plan documents are not used since every step is well known by all participants.

Correct Answer: D
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
A disaster recovery test should test the plan, processes, people, and IT systems. Therefore, if the plan is not used, its accuracy and adequacy cannot be verified. Disaster recovery should not rely on key staff since a disaster can occur when they are not available. It is common that not all systems can be tested in a limited test time frame. It is important, however, that those systems which are essential to the business are tested, and that the other systems are eventually tested throughout the year. One aim of the test is to identify and replace defective devices so that all systems can be replaced in the case of a disaster. Choice B would only be a concern if the number of discovered problems is systematically very high; in a real disaster, there is no need for a clean shutdown of the original production environment since the first priority is to bring the backup site up.

QUESTION 1000
The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan (DRP)?

- Contact information of key personnel
- Server inventory documentation
- Individual roles and responsibilities
- Procedures for declaring a disaster

Correct Answer: A
Section: BUSINESS CONTINUITY AND DISASTER RECOVERY
Explanation:
In the event of a disaster, it is important to have a current updated list of personnel who are key to the operation of the plan. Choices B, C, and D would be more likely to remain stable over time.