DOMAIN 4—INFORMATION SYSTEMS OPERATIONS AND BUSINESS RESILIENCE (23%)

A4-1 An organization is considering using a new IT service provider. From an audit perspective, which of the following would be the **MOST** important item to review?

A. References from other clients for the service provider
B. The physical security of the service provider site
C. The proposed service level agreement with the service provider
D. Background checks of the service provider's employees

C is the correct answer.

Justification:

A. A due diligence activity such as reviewing references from other clients is a good practice, but the service level agreement (SLA) would be most critical because it would define what specific levels of performance would be required and make the provider contractually obligated to deliver what was promised.
B. A due diligence activity such as reviewing physical security controls is a good practice, but the SLA would be most critical because it would define what specific levels of security would be required and make the provider contractually obligated to deliver what was promised.
C. **When contracting with a service provider, it is a good practice to enter into an SLA with the provider. An SLA is a guarantee that the provider will deliver the services according to the contract. The IS auditor will want to ensure that performance and security requirements are clearly stated in the SLA.**
D. A due diligence activity such as the use of background checks for the service provider's employees is a good practice, but the SLA would be most critical because it would define what specific levels of security and labor practices would be required and make the provider contractually obligated to deliver what was promised.

A4-2 An IS auditor is to assess the suitability of a service level agreement (SLA) between the organization and the supplier of outsourced services. To which of the following observations should the IS auditor pay the **MOST** attention? The SLA does not contain a:

A. transition clauses from the old supplier to a new supplier or back to internal in the case of expiration or termination.
B. late payment clause between the customer and the supplier.
C. contractual commitment for service improvement.
D. dispute resolution procedure between the contracting parties.

A is the correct answer.

Justification:

A. **The delivery of IT services for a specific customer always implies a close linkage between the client and the supplier of the service. If there are no contract terms to specify how the transition to a new supplier may be performed, there is the risk that the old supplier may simply "pull the plug" if the contract expires or is terminated or may not make data available to the outsourcing organization or new supplier. This would be the greatest risk to the organization.**
B. Contractual issues regarding payment, service improvement and dispute resolution are important but not as critical as ensuring that service disruption, data loss, data retention, or other significant events occur in the event that the organization switches to a new firm providing outsourced services.
C. The service level agreement (SLA) should address performance requirements and metrics to report on the status of services provided; it's nice to have commitment for performance improvement, although it's not mandated.
D. The SLA should address a dispute resolution procedure and specify the jurisdiction in case of a legal dispute, but this is not the most critical part of an SLA.

A4-3 An IS auditor reviewing a new outsourcing contract with a service provider would be **MOST** concerned if which of the following was missing?

A. A clause providing a "right to audit" the service provider
B. A clause defining penalty payments for poor performance
C. Predefined service level report templates
D. A clause regarding supplier limitation of liability

A is the correct answer.

Justification:

A. **The absence of a "right to audit" clause or other form of attestation that the supplier was compliant with a certain standard would potentially prevent the IS auditor from investigating any aspect of supplier performance moving forward, including control deficiencies, poor performance and adherence to legal requirements. This would be a major concern for the IS auditor because it would be difficult for the organization to assess whether the appropriate controls had been put in place.**
B. While a clear definition of penalty payment terms is desirable, not all contracts require the payment of penalties for poor performance, and when performance penalties are required, these penalties are often subject to negotiation on a case-by-case basis. As such, the absence of this information would not be as significant as a lack of right to audit.
C. While the inclusion of service level report templates would be desirable, as long as the requirement for service level reporting is included in the contract, the absence of predefined templates for reporting is not a significant concern.
D. The absence of a limitation of liability clause for the service provider would, theoretically, expose the provider to unlimited liability. This would be to the advantage of the outsourcing company so, while the IS auditor might highlight the absence of such a clause, it would not constitute a major concern.

A4-4 When reviewing the desktop software compliance of an organization, the IS auditor should be **MOST** concerned if the installed software:

A. was installed, but not documented in the IT department records.
B. was being used by users not properly trained in its use.
C. is not listed in the approved software standards document.
D. license will expire in the next 15 days.

C is the correct answer.

Justification:

A. All software, including licenses, should be documented in IT department records, but this is not as serious as the violation of policy in installing unapproved software.
B. Discovering that users have not been formally trained in the use of a software product is common, and while not ideal, most software includes help files and other tips that can assist in learning how to use the software effectively.
C. **The installation of software that is not allowed by policy is a serious violation and could put the organization at security, legal and financial risk. Any software that is allowed should be part of a standard software list. This is the first thing to review because this would also indicate compliance with policies.**
D. A software license that is about to expire is not a risk if there is a process in place to renew it.

A4-5 An IS auditor of a health care organization is reviewing contractual terms and conditions of a third-party cloud provider being considered to host patient health information. Which of the follow contractual terms would be the **GREATEST** risk to the customer organization?

A. Data ownership is retained by the customer organization.
B. The third-party provider reserves the right to access data to perform certain operations.
C. Bulk data withdrawal mechanisms are undefined.
D. The customer organization is responsible for backup, archive and restore.

B is the correct answer.

Justification:

A. The customer organization would want to retain data ownership and, therefore, this would not be a risk.
B. Some service providers reserve the right to access customer information (third-party access) to perform certain transactions and provide certain services. In the case of protected health information, regulations may restrict certain access. Organizations must review the regulatory environment in which the cloud provider operates because it may have requirements or restrictions of its own. Organizations must then determine whether the cloud provider provides appropriate controls to ensure that data are appropriately secure.
C. An organization may eventually wish to discontinue its service with a third-party cloud-based provider. The organization would then want to remove its data from the system and ensure that the service provider clears the system (including any backups) of its data. Some providers do not offer automated or bulk data withdrawal mechanisms, which the organization needs to migrate its data. These aspects should be clarified prior to using a third-party provider.
D. An organization may need to plan its own data recovery processes and procedures if the service provider does not make this available or the organization has doubts about the service provider's processes. This would only be a risk if the customer organization was unable to perform these activities itself.

A4-6 Which of the following recovery strategies is **MOST** appropriate for a business having multiple offices within a region and a limited recovery budget?

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

C is the correct answer.

Justification:

A. A hot site maintained by the business would be a costly solution but would provide a high degree of confidence.
B. Multiple cold sites leased for the multiple offices would lead to an ineffective solution with poor availability.
C. For a business having many offices within a region, a reciprocal arrangement among its offices would be most appropriate. Each office could be designated as a recovery site for some other office. This would be the least expensive approach and would provide an acceptable level of confidence.
D. A third-party facility for recovery is provided by a traditional hot site. This would be a costly approach providing a high degree of confidence.

A4-7 During an application audit, an IS auditor is asked to provide assurance of the database referential integrity. Which of the following should be reviewed?

A. Field definition
B. Master table definition
C. Composite keys
D. Foreign key structure

D is the correct answer.

Justification:

A. Field definitions describe the layout of the table but are not directly related to referential integrity.
B. Master table definition describes the structure of the database but is not directly related to referential integrity.
C. Composite keys describe how the keys are created but are not directly related to referential integrity.
D. Referential integrity in a relational database refers to consistency between coupled (linked) tables. Referential integrity is usually enforced by the combination of a primary key or candidate key (alternate key) and a foreign key. For referential integrity to hold, any field in a table that is declared a foreign key should contain only values from a parent table's primary key or a candidate key.

A4-8 An IS auditor is reviewing database security for an organization. Which of the following is the **MOST** important consideration for database hardening?

A. The default configurations are changed.
B. All tables in the database are denormalized.
C. Stored procedures and triggers are encrypted.
D. The service port used by the database server is changed.

A is the correct answer.

Justification:

A. Default database configurations, such as default passwords and services, need to be changed; otherwise, the database could be easily compromised by malicious code and by intruders.
B. The denormalization of a database is related more to performance than to security.
C. Limiting access to stored procedures is a valid security consideration but not as critical as changing default configurations.
D. Changing the service port used by the database is a component of the configuration changes that could be made to the database, but there are other more critical configuration changes that should be made first.

A4-9 In auditing a database environment, an IS auditor will be **MOST** concerned if the database administrator is performing which of the following functions?

A. Performing database changes according to change management procedures
B. Installing patches or upgrades to the operating system
C. Sizing table space and consulting on table join limitations
D. Performing backup and recovery procedures

B is the correct answer.

Justification:

A. Performing database changes according to change management procedures would be a normal function of the database administrator (DBA) and would be compliant with the procedures of the organization.
B. Installing patches or upgrades to the operating system is a function that should be performed by a systems administrator, not by a DBA. If a DBA were performing this function, there would be a risk based on inappropriate segregation of duties.
C. A DBA is expected to support the business through helping design, create and maintain databases and the interfaces to the databases.
D. The DBA often performs or supports database backup and recovery procedures.

A4-10 Which of the following is the **MOST** reasonable option for recovering a non-critical system?

A. Warm site
B. Mobile site
C. Hot site
D. Cold site

D is the correct answer.

Justification:

A. A warm site is generally available at a medium cost, requires less time to become operational and is suitable for sensitive operations that should be recovered in a moderate amount of time.
B. A mobile site is a vehicle ready with all necessary computer equipment that can be moved to any location, depending upon the need. The need for a mobile site depends upon the scale of operations.
C. A hot site is contracted for a shorter time period at a higher cost, and it is better suited for recovery of vital and critical applications.
D. Generally, a cold site is contracted for a longer period at a lower cost. Because it requires more time to make a cold site operational, it is generally used for noncritical applications.

A4-11 An IS auditor is evaluating the effectiveness of the change management process in an organization. What is the **MOST** important control that the IS auditor should look for to ensure system availability?

A. Changes are authorized by IT managers at all times.
B. User acceptance testing is performed and properly documented.
C. Test plans and procedures exist and are closely followed.
D. Capacity planning is performed as part of each development project.

C is the correct answer.

Justification:
A. Changes are usually required to be signed off by a business analyst, member of the change control board or other authorized representative, not necessarily by IT management.
B. User acceptance testing is important but not a critical element of change control and would not usually address the topic of availability as asked in the question.
C. The most important control for ensuring system availability is to implement a sound test plan and procedures that are followed consistently.
D. While capacity planning should be considered in each development project, it will not ensure system availability, nor is it part of the change control process.

A4-12 Data flow diagrams are used by IS auditors to:

A. identify key controls.
B. highlight high-level data definitions.
C. graphically summarize data paths and storage.
D. portray step-by-step details of data generation.

C is the correct answer.

Justification:
A. Identifying key controls is not the focus of data flow diagrams. The focus is as the name states—flow of data.
B. A data dictionary may be used to document data definitions, but the data flow diagram is used to document how data move through a process.
C. Data flow diagrams are used as aids to graph or chart data flow and storage. They trace data from their origination to destination, highlighting the paths and storage of data.
D. The purpose of a data flow diagram is to track the movement of data through a process and is not primarily to document or indicate how data are generated.

A4-13 Which of the following statements is useful while drafting a disaster recovery plan?

A. Downtime costs decrease as the recovery point objective increases.
B. Downtime costs increase with time.
C. Recovery costs are independent of time.
D. Recovery costs can only be controlled on a short-term basis.

B is the correct answer.

Justification:
A. Downtime costs are not related to the recovery point objective (RPO). The RPO defines the data backup strategy, which is related to recovery costs rather than to downtime costs.
B. Downtime costs—such as loss of sales, idle resources, salaries—increase with time. A disaster recovery plan should be drawn to achieve the lowest downtime costs possible.
C. Recovery costs decrease with the time allowed for recovery. For example, recovery costs to recover business operations within two days will be higher than the cost to recover business within seven days. The essence of an effective DRP is to minimize uncertainty and increase predictability.
D. With good planning, recovery costs can be predicted and contained.

A4-14 Although management has stated otherwise, an IS auditor has reasons to believe that the organization is using software that is not licensed. In this situation, the IS auditor should **FIRST**:

A. include the statement from management in the audit report.
B. verify the software is in use through testing.
C. include the item in the audit report.
D. discuss the issue with senior management because it could have a negative impact on the organization.

B is the correct answer.

Justification:
A. The statement from management may be included in the audit report, but the auditor should independently validate the statements made by management to ensure completeness and accuracy.
B. When there is an indication that an organization might be using unlicensed software, the IS auditor should obtain sufficient evidence before including it in report.
C. With respect to this matter, representations obtained from management cannot be independently verified.
D. If the organization is using software that is not licensed, the IS auditor, to maintain objectivity and independence, must include this in the report, but the IS auditor should verify that this is in fact the case before presenting it to senior management.

A4-15 An advantage of using unshielded twisted-pair (UTP) cable for data communication over other copper-based cables is that UTP cable:

A. reduces crosstalk between pairs.
B. provides protection against wiretapping.
C. can be used in long-distance networks.
D. is simple to install.

A is the correct answer.

Justification:
A. The use of unshielded twisted-pair (UTP) in copper will reduce the likelihood of crosstalk.
B. While the twisted nature of the media will reduce sensitivity to electromagnetic disturbances, an unshielded copper wire does not provide adequate protection against wiretapping.
C. Attenuation sets in if copper twisted-pair cable is used for longer than 100 meters, necessitating the use of a repeater.
D. The tools and techniques to install UTP are not simpler or easier than other copper-based cables.

A4-16 Which of the following is the **MOST** critical element to effectively execute a disaster recovery plan?

A. Offsite storage of backup data
B. Up-to-date list of key disaster recovery contacts
C. Availability of a replacement data center
D. Clearly defined recovery time objective

A is the correct answer.

Justification:
A. Remote storage of backups is the most critical disaster recovery plan (DRP) element of the items listed because access to backup data is required to restore systems.
B. Having a list of key contacts is important but not as important as having adequate data backup.
C. A DRP may use a replacement data center or some other solution such as a mobile site, reciprocal agreement or outsourcing agreement.
D. Having a clearly defined recovery time objective is especially important for business continuity planning, but the core element of disaster recovery (the recovery of IT infrastructure and capability) is data backup.

A4-17 While reviewing the process for continuous monitoring of the capacity and performance of IT resources, an IS auditor should **PRIMARILY** ensure that the process is focused on:

A. adequately monitoring service levels of IT resources and services.
B. providing data to enable timely planning for capacity and performance requirements.
C. providing accurate feedback on IT resource capacity.
D. properly forecasting performance, capacity and throughput of IT resources.

C is the correct answer.

Justification:

A. Continuous monitoring helps to ensure that service level agreements (SLAs) are met, but this would not be the primary focus of monitoring. It is possible that even if a system were offline, it would meet the requirements of an SLA. Therefore, accurate availability monitoring is more important.
B. While data gained from capacity and performance monitoring would be an input to the planning process, the primary focus would be to monitor availability.
C. Accurate capacity monitoring of IT resources would be the most critical element of a continuous monitoring process.
D. While continuous monitoring would help management to predict likely IT resource capabilities, the more critical issue would be that availability monitoring is accurate.

A4-18 Which of the following groups is the **BEST** source of information for determining the criticality of application systems as part of a business impact analysis?

A. Business processes owners
B. IT management
C. Senior business management
D. Industry experts

A is the correct answer.

Justification:

A. Business process owners have the most relevant information to contribute because the business impact analysis (BIA) is designed to evaluate criticality and recovery time lines, based on business needs.
B. While IT management must be involved, they may not be fully aware of the business processes that need to be protected.
C. While senior management must be involved, they may not be fully aware of the criticality of applications that need to be protected.
D. The BIA is dependent on the unique business needs of the organization and the advice of industry experts is of limited value.

A4-19 An IS auditor is reviewing an organization's disaster recovery plan (DRP) implementation. The project was completed on time and on budget. During the review, the auditor uncovers several areas of concern. Which of the following presents the **GREATEST** risk?

A. Testing of the DRP has not been performed.
B. The disaster recovery strategy does not specify use of a hot site.
C. The business impact analysis was conducted, but the results were not used.
D. The disaster recovery project manager for the implementation has recently left the organization.

C is the correct answer.

Justification:

A. Although testing a disaster recovery plan (DRP) is a critical component of a successful disaster recovery strategy, this is not the biggest risk; the biggest risk comes from a plan that is not properly designed.
B. Use of a hot site is a strategic determination based on tolerable downtime, cost and other factors. Although using a hot site may be considered a good practice, this is a very costly solution that may not be required for the organization.
C. **The risk of not using the results of the business impact analysis (BIA) for disaster recovery planning means that the DRP may not be designed to recover the most critical assets in the correct order. As a result, the plan may not be adequate to allow the organization to recover from a disaster.**
D. If the DRP is designed and documented properly, the loss of an experienced project manager should have minimal impact. The risk of a poorly designed plan that may not meet the requirements of the business is much more significant than the risk posed by loss of the project manager.

A4-20 A vendor has released several critical security patches over the past few months and this has put a strain on the ability of the administrators to keep the patches tested and deployed in a timely manner. The administrators have asked if they could reduce the testing of the patches. What approach should the organization take?

A. Continue the current process of testing and applying patches.
B. Reduce testing and ensure that an adequate backout plan is in place.
C. Delay patching until resources for testing are available.
D. Rely on the vendor's testing of the patches.

A is the correct answer.

Justification:

A. **Applying security software patches promptly is critical to maintain the security of the servers; further, testing the patches is important because the patches may affect other systems and business operations. Because the vendor has recently released several critical patches in a short time, it can be hoped that this is a temporary problem and does not need a revision to policy or procedures.**
B. Reduced testing increases the risk of business operation disruption due to a faulty or incompatible patch. While a backout plan does help mitigate this risk, a thorough testing up front would be the more appropriate option.
C. Applying security software patches promptly is critical to maintain the security of the servers. Delaying patching would increase the risk of a security breach due to system vulnerability.
D. The testing done by the vendor may not be applicable to the systems and environment of the organization that needs to deploy the patches.

A4-21 Which of the following issues should be a **MAJOR** concern to an IS auditor who is reviewing a service level agreement (SLA)?

A. A service adjustment resulting from an exception report took a day to implement.
B. The complexity of application logs used for service monitoring made the review difficult.
C. Service measures were not included in the SLA.
D. The document is updated on an annual basis.

C is the correct answer.

Justification:
A. Resolving issues related to exception reports is an operational issue that should be addressed in the service level agreement (SLA); however, a response time of one day may be acceptable depending on the terms of the SLA.
B. The complexity of application logs is an operational issue, which is not related to the SLA.
C. **Lack of service measures will make it difficult to gauge the efficiency and effectiveness of the IT services being provided.**
D. While it is important that the document be current, depending on the term of the agreement, it may not be necessary to change the document more frequently than annually.

A4-22 During an IS audit of the disaster recovery plan of a global enterprise, the auditor observes that some remote offices have very limited local IT resources. Which of the following observations would be the **MOST** critical for the IS auditor?

A. A test has not been made to ensure that local resources could maintain security and service standards when recovering from a disaster or incident.
B. The corporate business continuity plan does not accurately document the systems that exist at remote offices.
C. Corporate security measures have not been incorporated into the test plan.
D. A test has not been made to ensure that tape backups from the remote offices are usable.

A is the correct answer.

Justification:
A. **Regardless of the capability of local IT resources, the most critical risk would be the lack of testing, which would identify quality issues in the recovery process.**
B. The corporate business continuity plan may not include disaster recovery plan (DRP) details for remote offices. It is important to ensure that the local plans have been tested.
C. Security is an important issue because many controls may be missing during a disaster. However, not having a tested plan is more important.
D. The backups cannot be trusted until they have been tested. However, this should be done as part of the overall tests of the DRP.

A4-23 Which of the following reports should an IS auditor use to check compliance with a service level agreement's requirement for uptime?

A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports

D is the correct answer.

Justification:

A. Utilization reports document the use of computer equipment, and can be used by management to predict how, where and/or when resources are required.
B. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. These error reports may not indicate actual system uptime.
C. System logs are used for recording the system's activities. They may not indicate availability.
D. IS inactivity, such as downtime, is addressed by availability reports. These reports provide the time periods during which the computer was available for utilization by users or other processes.

A4-24 Which of the following would an IS auditor use to determine if unauthorized modifications were made to production programs?

A. System log analysis
B. Compliance testing
C. Forensic analysis
D. Analytical review

B is the correct answer.

Justification:

A. System log analysis would identify changes and activity on a system but would not identify whether the change was authorized unless conducted as a part of a compliance test.
B. Determining that only authorized modifications are made to production programs would require the change management process be reviewed to evaluate the existence of a trail of documentary evidence. Compliance testing would help to verify that the change management process has been applied consistently.
C. Forensic analysis is a specialized technique for criminal investigation.
D. An analytical review assesses the general control environment of an organization.

A4-25 During a change control audit of a production system, an IS auditor finds that the change management process is not formally documented and that some migration procedures failed. What should the IS auditor do next?

A. Recommend redesigning the change management process.
B. Gain more assurance on the findings through root cause analysis.
C. Recommend that program migration be stopped until the change process is documented.
D. Document the finding and present it to management.

B is the correct answer.

Justification:
A. While it may be necessary to redesign the change management process, this cannot be done until a root cause analysis is conducted to determine why the current process is not being followed.
B. A change management process is critical to IT production systems. Before recommending that the organization take any other action (e.g., stopping migrations, redesigning the change management process), the IS auditor should gain assurance that the incidents reported are related to deficiencies in the change management process and not caused by some process other than change management.
C. A business relies on being able to make changes when necessary, and security patches must often be deployed promptly. It would not be feasible to halt all changes until a new process is developed.
D. The results of the audit including the findings of noncompliance will be delivered to management once a root cause analysis of the issue has been completed.

A4-26 An IS auditor evaluating the resilience of a high-availability network should be **MOST** concerned if:

A. the setup is geographically dispersed.
B. the servers are clustered in one site.
C. a hot site is ready for activation.
D. diverse routing is implemented for the network.

B is the correct answer.

Justification:
A. Dispersed geographic locations provide backup if a site has been destroyed.
B. A clustered setup in one site makes the entire network vulnerable to natural disasters or other disruptive events.
C. A hot site would also be a good alternative for a single point-of-failure site.
D. Diverse routing provides telecommunications backup if a network is not available.

A4-27 Management considered two projections for its disaster recovery plan: plan A with two months to fully recover and plan B with eight months to fully recover. The recovery point objectives are the same in both plans. It is reasonable to expect that plan B projected higher:

A. downtime costs.
B. resumption costs.
C. recovery costs.
D. walk-through costs.

A is the correct answer.

Justification:
A. Because management considered a longer time window for recovery in plan B, downtime costs included in the plan are likely to be higher.
B. Because the recovery time for plan B is longer, resumption costs can be expected to be lower.
C. Because the recovery time for plan B is longer, recovery costs can be expected to be lower.
D. Walk-through costs are not a part of disaster recovery.

A4-28 Which of the following would an IS auditor consider to be **MOST** helpful when evaluating the effectiveness and adequacy of a preventive computer maintenance program?

A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule

A is the correct answer.

Justification:

A. A system downtime log provides evidence regarding the effectiveness and adequacy of computer preventive maintenance programs. The log is a detective control, but because it is validating the effectiveness of the maintenance program, it is validating a preventive control.
B. Vendor's reliability figures are not an effective measure of a preventive maintenance program.
C. Reviewing the log is a good detective control to ensure that maintenance is being done; however, only the system downtime will indicate whether the preventive maintenance is actually working well.
D. A schedule is a good control to ensure that maintenance is scheduled and that no items are missed in the maintenance schedule; however, it is not a guarantee that the work is actually being done.

A4-29 An organization has implemented an online customer help desk application using a software as a service (SaaS) operating model. An IS auditor is asked to recommend the best control to monitor the service level agreement (SLA) with the SaaS vendor as it relates to availability. What is the **BEST** recommendation that the IS auditor can provide?

A. Ask the SaaS vendor to provide a weekly report on application uptime.
B. Implement an online polling tool to monitor the application and record outages.
C. Log all application outages reported by users and aggregate the outage time weekly.
D. Contract an independent third party to provide weekly reports on application uptime.

B is the correct answer.

Justification:

A. Weekly application availability reports are useful, but these reports represent only the vendor's perspective. While monitoring these reports, the organization can raise concerns of inaccuracy; however, without internal monitoring, such concerns cannot be substantiated.
B. Implementing an online polling tool to monitor and record application outages is the best option for an organization to monitor the software as a service application availability. Comparing internal reports with the vendor's service level agreement (SLA) reports would ensure that the vendor's monitoring of the SLA is accurate and that all conflicts are appropriately resolved.
C. Logging the outage times reported by users is helpful but does not give a true picture of all outages of the online application. Some outages may go unreported, especially if the outages are intermittent.
D. Contracting a third party to implement availability monitoring is not a cost-effective option. Additionally, this results in a shift from monitoring the SaaS vendor to monitoring the third party.

A4-30 Applying a retention date on a file will ensure that:

A. data cannot be read until the date is set.
B. data will not be deleted before that date.
C. backup copies are not retained after that date.
D. datasets having the same name are differentiated.

B is the correct answer.

Justification:
A. The retention date will not affect the ability to read the file.
B. A retention date will ensure that a file cannot be overwritten or deleted before that date has passed.
C. Backup copies would be expected to have a different retention date and, therefore, may be retained after the file has been overwritten.
D. The creation date, not the retention date, will differentiate files with the same name.

A4-31 Which of the following is a network diagnostic tool that monitors and records network information?

A. Online monitor
B. Downtime report
C. Help desk report
D. Protocol analyzer

D is the correct answer.

Justification:
A. Online monitors measure telecommunication transmissions and determine whether transmissions were accurate and complete.
B. Downtime reports track the availability of telecommunication lines and circuits.
C. Help desk reports are prepared by the help desk, which is staffed or supported by IS technical support personnel trained to handle problems occurring during the course of IS operations.
D. Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached.

A4-32 An IS auditor needs to review the procedures used to restore a software application to its state prior to an upgrade. Therefore, the auditor needs to assess:

A. problem management procedures.
B. software development procedures.
C. backout procedures.
D. incident management procedures.

C is the correct answer.

Justification:
A. Problem management procedures are used to track user feedback and issues related to the operation of an application for trend analysis and problem resolution.
B. Software development procedures such as the software development life cycle (SDLC) are used to manage the creation or acquisition of new or modified software.
C. Backout procedures are used to restore a system to a previous state and are an important element of the change control process. The other choices are not related to the change control process—a process which specifies what procedures should be followed when software is being upgraded but the upgrade does not work and requires a fallback to its former state.
D. Incident management procedures are used to manage errors or problems with system operation. They are usually used by a help desk. One of the incident management procedures may be how to follow a fallback plan.

A4-33 Which of the following is a **MAJOR** concern during a review of help desk activities?

A. Certain calls could not be resolved by the help desk team.
B. A dedicated line is not assigned to the help desk team.
C. Resolved incidents are closed without reference to end users.
D. The help desk instant messaging has been down for more than six months.

C is the correct answer.

Justification:
A. Although this is of concern, it should be expected. A problem escalation procedure should be developed to handle such scenarios.
B. Ideally, a help desk team should have dedicated lines, but this exception is not as serious as the technical team unilaterally closing an incident.
C. **The help desk function is a service-oriented unit. The end users must be advised before an incident can be regarded as closed.**
D. Instant messaging is an add-on to improve the effectiveness of the help desk team. Its absence cannot be seen as a major concern as long as calls can still be made.

A4-34 The **MAIN** purpose for periodically testing offsite disaster recovery 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.

C is the correct answer.

Justification:
A. The testing of an offsite facility does nothing to protect the integrity of the database. It may test the validity of backups but does not protect their integrity.
B. Testing an offsite location validates the value of the contingency plans and is not used to eliminate detailed plans.
C. **The main purpose of offsite hardware testing is to ensure the continued compatibility of the contingency facilities so that assurance can be gained that the contingency plans would work in an actual disaster.**
D. Program and system documentation should be reviewed continuously for currency. A test of an offsite facility may ensure that the documentation for that site is current, but this is not the purpose of testing an offsite facility.

A4-35 A large chain of shops with electronic funds transfer 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

D is the correct answer.

Justification:

A. Offsite storage of backups would not help, because electronic funds transfer tends to be an online process and offsite storage will not replace the dysfunctional processor.
B. 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 and may require technical expertise to cutover to the alternate equipment.
C. Installation of duplex communication links would be most appropriate if it were only the communication link that failed.
D. 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 of the shops. This could be caused by failure of equipment, power or communications.

A4-36 The database administrator suggests that database efficiency can be improved by denormalizing some tables. This would result in:

A. loss of confidentiality.
B. increased redundancy.
C. unauthorized accesses.
D. application malfunctions.

B is the correct answer.

Justification:

A. Denormalization should not cause loss of confidentiality even though confidential data may be involved. The database administrator should ensure that access controls to the databases remain effective.
B. Normalization is a design or optimization process for a relational database that increases redundancy. Redundancy, which is usually considered positive when it is a question of resource availability, is negative in a database environment because it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons.
C. Denormalization pertains to the structure of the database, not the access controls. It should not result in unauthorized access.
D. Denormalization may require some changes to the calls between databases and applications but should not cause application malfunctions.

A4-37 An IS auditor has been assigned to conduct a test that compares job run logs to computer job schedules. Which of the following observations would be of the **GREATEST** concern to the IS auditor?

A. There are a growing number of emergency changes.
B. There were instances when some jobs were not completed on time.
C. There were instances when some jobs were overridden by computer operators.
D. Evidence shows that only scheduled jobs were run.

C is the correct answer.

Justification:
A. Emergency changes are acceptable as long as they are properly documented as part of the process.
B. Instances of jobs not being completed on time is a potential issue and should be investigated, but it is not the greatest concern.
C. **The overriding of computer processing jobs by computer operators could lead to unauthorized changes to data or programs. This is a control concern; thus, it is always critical.**
D. The audit should find that all scheduled jobs were run and that any exceptions were documented. This would not be a violation.

A4-38 A new business requirement required changing database vendors. Which of the following areas should the IS auditor **PRIMARILY** examine in relation to this implementation?

A. Integrity of the data
B. Timing of the cutover
C. Authorization level of users
D. Normalization of the data

A is the correct answer.

Justification:
A. **A critical issue when migrating data from one database to another is the integrity of the data and ensuring that the data are migrated completely and correctly.**
B. The timing of the cutover is important, but because the data are being migrated to a new database, duplication should not be an issue.
C. The authorization of the users is not as relevant as the authorization of the application because the users will interface with the database through an application, and the users will not directly interface with the database.
D. Normalization is used to design the database and is not necessarily related to database migration.

A4-39 The objective of concurrency control in a database system is to:

A. restrict updating of the database to authorized users.
B. ensure integrity when two processes attempt to update the same data at the same time.
C. prevent inadvertent or unauthorized disclosure of data in the database.
D. ensure the accuracy, completeness and consistency of data.

B is the correct answer.

Justification:
A. Access controls restrict updating of the database to authorized users.
B. **Concurrency controls prevent data integrity problems, which can arise when two update processes access the same data item at the same time.**
C. Controls such as passwords prevent the inadvertent or unauthorized disclosure of data from the database.
D. Quality controls such as edits ensure the accuracy, completeness and consistency of data maintained in the database.

A4-40 Which of the following controls would provide the **GREATEST** assurance of database integrity?

A. Audit log procedures
B. Table link/reference checks
C. Query/table access time checks
D. Rollback and rollforward database features

B is the correct answer.

Justification:

A. Audit log procedures enable recording of all events that have been identified and help in tracing the events. However, they only point to the event and do not ensure completeness or accuracy of the database contents.
B. Performing table link/reference checks serves to detect table linking errors (such as completeness and accuracy of the contents of the database), and thus provides the greatest assurance of database integrity.
C. Querying/monitoring table access time checks helps designers improve database performance but not integrity.
D. Rollback and rollforward database features ensure recovery from an abnormal disruption. They assure the integrity of the transaction that was being processed at the time of disruption, but do not provide assurance on the integrity of the contents of the database.

A4-41 Which of the following is widely accepted as one of the critical components in networking management?

A. Configuration and change management
B. Topological mappings
C. Application of monitoring tools
D. Proxy server troubleshooting

A is the correct answer.

Justification:

A. Configuration management is widely accepted as one of the key components of any network because it establishes how the network will function internally and externally. It also deals with the management of configuration and monitoring performance. Change management ensures that the setup and management of the network is done properly, including managing changes to the configuration, removal of default passwords and possibly hardening the network by disabling unneeded services.
B. Topological mappings provide outlines of the components of the network and its connectivity. This is important to address issues such as single points of failure and proper network isolation but is not the most critical component of network management.
C. Application monitoring is not a critical part of network management.
D. Proxy server troubleshooting is used for troubleshooting purposes, and managing a proxy is only a small part of network management.

A4-42 In evaluating programmed controls over password management, which of the following is the IS auditor **MOST** likely to rely on?

A. A size check
B. A hash total
C. A validity check
D. A field check

C is the correct answer.

Justification:

A. A size check is useful because passwords should have a minimum length, but it is not as strong of a control as validity.
B. Passwords are not typically entered in a batch mode, so a hash total would not be effective. More important, a system should not accept incorrect values of a password, so a hash total as a control will not indicate any weak passwords, errors or omissions.
C. **A validity check would be the most useful for the verification of passwords because it would verify that the required format has been used—for example, not using a dictionary word, including non-alphabetical characters, etc. An effective password must have several different types of characters: alphabetical, numeric and special.**
D. The implementation of a field check would not be as effective as a validity check that verifies that all password criteria have been met.

A4-43 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 live tested.
D. The security infrastructures in each company may be different.

A is the correct answer.

Justification:

A. **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.**
B. 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.
C. The plan can be tested by paper-based walk-throughs and possibly by agreement between the companies.
D. The difference in security infrastructures, while a risk, is not insurmountable.

A4-44 Which of the following is **MOST** directly affected by network performance monitoring tools?

A. Integrity
B. Availability
C. Completeness
D. Confidentiality

B is the correct answer.

Justification:

A. Network monitoring tools can be used to detect errors that are propagating through a network, but their primary focus is on network reliability so that the network is available when required.
B. Network monitoring tools allow observation of network performance and problems. This allows the administrator to take corrective action when network problems are observed. Therefore, the characteristic that is most directly affected by network monitoring is availability.
C. Network monitoring tools will not measure completeness of the communication. This is measured by the end points in the communication.
D. A network monitoring tool can violate confidentiality by allowing a network administrator to observe non-encrypted traffic. This requires careful protection and policies regarding the use of network monitoring tools.

A4-45 When auditing the onsite archiving process of emails, the IS auditor should pay the **MOST** attention to:

A. the existence of a data retention policy.
B. the storage capacity of the archiving solution.
C. the level of user awareness concerning email use.
D. the support and stability of the archiving solution manufacturer.

A is the correct answer.

Justification:

A. Without a data retention policy that is aligned to the company's business and compliance requirements, the email archive may not preserve and reproduce the correct information when required.
B. The storage capacity of the archiving solution would be irrelevant if the proper email messages have not been properly preserved and others have been deleted.
C. The level of user awareness concerning email use would not directly affect the completeness and accuracy of the archived email.
D. The support and stability of the archiving solution manufacturer is secondary to the need to ensure a retention policy. Vendor support would not directly affect the completeness and accuracy of the archived email.

A4-46 Vendors have released patches fixing security flaws in their software. Which of the following should an IS auditor recommend in this situation?

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

A is the correct answer.

Justification:

A. **The effect of installing the patch should be immediately evaluated and installation should occur based on the results of the evaluation. There are numerous cases where a patch from one vendor has affected other systems; therefore, it is necessary to test the patches as much as possible before rolling them out to the entire organization.**
B. New software versions with all fixes included are not always available and a full installation could be time consuming.
C. To install the patch without knowing what it might affect could easily cause problems. The installation of a patch may also affect system availability; therefore, the patch should be rolled out at a time that is acceptable to the business.
D. Declining to deal with vendors does not take care of the flaw and may severely limit service options.

A4-47 Which of the following controls would be **MOST** effective in ensuring that production source code and object code are synchronized?

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

D is the correct answer.

Justification:

A. Using version control software and comparing source and object code is a good practice but may not detect a problem where the source code is a different version than the object code.
B. All production libraries should be protected with access controls, and this may protect source code from tampering. However, this will not ensure that source and object codes are based on the same version.
C. It is a good practice to protect all source and object code—even in development. However, this will not ensure the synchronization of source and object code.
D. **Date and time-stamp reviews of source and object code would ensure that source code, which has been compiled, matches the production object code. This is the most effective way to ensure that the approved production source code is compiled and is the one being used.**

A4-48 A database administrator (DBA) who needs to make emergency changes to a database after normal working hours should log in:

A. with their named account to make the changes.
B. with the shared DBA account to make the changes.
C. to the server administrative account to make the changes.
D. to the user's account to make the changes.

A is the correct answer.

Justification:

A. Logging in using the named user account before using the database administrator (DBA) account provides accountability by noting the person making the changes.
B. The DBA account is typically a shared user account. The shared account makes it difficult to establish the identity of the support user who is performing the database update.
C. The server administrative accounts are shared and may be used by multiple support users. In addition, the server privilege accounts may not have the ability to perform database changes.
D. The use of a normal user account would not have sufficient privileges to make changes on the database.

A4-49 During an assessment of software development practices, an IS auditor finds that open source software components were used in an application designed for a client. What is the **GREATEST** concern the auditor would have about the use of open source software?

A. The client did not pay for the open source software components.
B. The organization and client must comply with open source software license terms.
C. Open source software has security vulnerabilities.
D. Open source software is unreliable for commercial use.

B is the correct answer.

Justification:

A. A major benefit of using open source software is that it is free. The client is not required to pay for the open source software components; however, both the developing organization and the client should be concerned about the licensing terms and conditions of the open source software components that are being used.
B. There are many types of open source software licenses and each has different terms and conditions. Some open source software licensing allows use of the open source software component freely but requires that the completed software product must also allow the same rights. This is known as viral licensing, and if the development organization is not careful, its products could violate licensing terms by selling the product for profit. The IS auditor should be most concerned with open source software licensing compliance to avoid unintended intellectual property risk or legal consequences.
C. Open source software, just like any software code, should be tested for security flaws and should be part of the normal system development life cycle (SDLC) process. This is not more of a concern than licensing compliance.
D. Open source software does not inherently lack quality. Like any software code, it should be tested for reliability and should be part of the normal SDLC process. This is not more of a concern than licensing compliance.

A4-50 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?

A. Allow changes to be made only with the database administrator (DBA) user account
B. Make changes to the database after granting access to a normal user account
C. Use the DBA user account to make changes, log the changes and review the change log the following day
D. Use the normal user account to make changes, log the changes and review the change log the following day

C is the correct answer.

Justification:

A. The use of the database administrator (DBA) user account without logging would permit uncontrolled changes to be made to databases after access to the account was obtained.
B. A normal user account should not have access to a database. This would permit uncontrolled changes to any of the databases.
C. **The use of a DBA user account is normally set up to log all changes made and is most appropriate for changes made outside of normal hours. The use of a log, which records the changes, allows changes to be reviewed. Because an abbreviated number of steps are used, this represents an adequate set of compensating controls.**
D. Users should not be able to make changes. Logging would only provide information on changes made but would not limit changes to only those who were authorized.

A4-51 Which of the following tests performed by an IS auditor would be the **MOST** effective in determining compliance with change control procedures in an organization?

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

B is the correct answer.

Justification:

A. Software migration records may not have all changes listed—changes could have been made that were not included in the migration records.
B. **The most effective method is to determine what changes have been made (check logs and modified dates) and then verify that they have been approved.**
C. Change control records may not have all changes listed.
D. Ensuring that only appropriate staff can migrate changes into production is a key control process but, in itself, does not verify compliance.

A4-52 When an organization's disaster recovery plan has a reciprocal agreement, which of the following risk treatment approaches is being applied?

A. Transfer
B. Mitigation
C. Avoidance
D. Acceptance

B is the correct answer.

Justification:

A. Risk transfer is the transference of risk to a third party (e.g., buying insurance for activities that pose a risk).
B. A reciprocal agreement in which two organizations agree to provide computing resources to each other in the event of a disaster is a form of risk mitigation. This usually works well if both organizations have similar information processing facilities. Because the intended effect of reciprocal agreements is to have a functional disaster recovery plan, it is a risk mitigation strategy.
C. Risk avoidance is the decision to cease operations or activities that give rise to a risk. For example, a company may stop accepting credit card payments to avoid the risk of credit card information disclosure.
D. Risk acceptance occurs when an organization decides to accept the risk as it is and to do nothing to mitigate or transfer it.

A4-53 A programmer maliciously modified a production program to change data and then restored it back to the original code. Which of the following would **MOST** effectively detect the malicious activity?

A. Comparing source code
B. Reviewing system log files
C. Comparing object code
D. Reviewing executable and source code integrity

B is the correct answer.

Justification:

A. Source code comparisons are ineffective because the original programs were restored, and the changed program does not exist.
B. Reviewing system log files is the only trail that may provide information about the unauthorized activities in the production library.
C. Object code comparisons are ineffective because the original programs were restored, and the changed program does not exist.
D. Reviewing executable and source code integrity is an ineffective control, because the source code was changed back to the original and will agree with the current executable.

A4-54 An IS auditor is reviewing an organization's recovery from a disaster in which not all the critical data needed to resume business operations were retained. Which of the following was incorrectly defined?

A. The interruption window
B. The recovery time objective
C. The service delivery objective
D. The recovery point objective

D is the correct answer.

Justification:

A. The interruption window is defined as the amount of time during which the organization is unable to maintain operations from the point of failure to the time that the critical services/applications are restored.
B. The recovery time objective is determined based on the acceptable downtime in the case of a disruption of operations.
C. The service delivery objective (SDO) is directly related to the business needs. SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.
D. The recovery point objective (RPO) is determined based on the acceptable data loss in the case of a disruption of operations. RPO defines the point in time from which it is necessary to recover the data and quantifies, in terms of time, the permissible amount of data loss in the case of interruption.

A4-55 The **PRIMARY** benefit of an IT manager monitoring technical capacity is to:

A. identify the need for new hardware and storage procurement.
B. determine the future capacity need based on usage.
C. ensure that the service level requirements are met.
D. ensure that systems operate at optimal capacity.

C is the correct answer.

Justification:

A. This is one benefit of monitoring technical capacity because it can help forecast future demands, not just react to system failures. However, the primary responsibility of the IT manager is to meet the overall requirement to ensure that IT is meeting the service level expectations of the business.
B. Determining future capacity is one definite benefit of technical capability monitoring.
C. Capacity monitoring has multiple objectives; however, the primary objective is to ensure compliance with the internal service level agreement between the business and IT.
D. IT management is interested in ensuring that systems are operating at optimal capacity, but their primary obligation is to ensure that IT is meeting the service level requirements of the business.

A4-56 An IS auditor reviewing an organization's disaster recovery plan should **PRIMARILY** verify that it is:

A. tested every six months.
B. regularly reviewed and updated.
C. approved by the chief executive officer.
D. communicated to every department head in the organization.

B is the correct answer.

Justification:

A. The plan must be subjected to regular testing, but the period between tests will depend on the nature of the organization, the amount of change in the organization and the relative importance of IS. Three months, or even annually, may be appropriate in different circumstances.
B. The plan should be reviewed at appropriate intervals, depending on the nature of the business and the rate of change of systems and personnel. Otherwise, it may become out of date and may no longer be effective.
C. Although the disaster recovery plan should receive the approval of senior management, it need not be the chief executive officer if another executive officer is equally or more appropriate. For a purely IS-related plan, the executive responsible for technology may have approved the plan.
D. Although a business continuity plan is likely to be circulated throughout an organization, the IS disaster recovery plan will usually be a technical document and only relevant to IS and communication staff.

A4-57 There are several methods of providing telecommunication 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.

B is the correct answer.

Justification:

A. Alternative routing is a method of routing information via an alternate medium such as copper cable or fiber optics. This involves the use of different networks, circuits or end points should the normal network be unavailable.
B. Diverse routing routes traffic through split-cable facilities or duplicate-cable facilities. This can be accomplished with different and/or duplicate cable sheaths. If different cable sheaths are used, the cable may be in the same conduit and, therefore, subject to the same interruptions as the cable it is backing up. The communication service subscriber can duplicate the facilities by having alternate routes, although the entrance to and from the customer premises may be in the same conduit. The subscriber can obtain diverse routing and alternate routing from the local carrier, including dual-entrance facilities. This type of access is time consuming and costly.
C. Long-haul network diversity is a diverse, long-distance network using different packet switching circuits among the major long-distance carriers. It ensures long-distance access should any carrier experience a network failure.
D. Last-mile circuit protection is a redundant combination of local carrier T-1s (E-1s in Europe), microwave and/or coaxial cable access to the local communications loop. This enables the facility to have access during a local carrier communication disaster. Alternate local-carrier routing is also used.

A4-58 Recovery procedures for an information processing facility are **BEST** based on:

A. recovery time objective.
B. recovery point objective.
C. maximum tolerable outage.
D. information security policy.

A is the correct answer.

Justification:

A. **The recovery time objective (RTO). is the amount of time allowed for the recovery of a business function or resource after a disaster occurs; the RTO is the desired recovery time frame based on maximum tolerable outage (MTO) and available recovery alternatives.**
B. The recovery point objective (RPO) has the greatest influence on the recovery strategies for given data. It is determined based on the acceptable data loss in case of a disruption of operations. The RPO effectively quantifies the permissible amount of data loss in case of interruption.
C. MTO is the amount of time allowed for the recovery of a business function or resource after a disaster occurs; it represents the time by which the service must be restored before the organization is faced with the threat of collapse.
D. An information security policy does not address recovery procedures.

A4-59 An IS auditor is performing an audit in the data center when the fire alarm begins sounding. The audit scope includes disaster recovery, so the auditor observes the data center staff respond to the alarm. Which of the following is the **MOST** important action for the data center staff to complete in this scenario?

A. Notify the local fire department of the alarm condition.
B. Prepare to activate the fire suppression system.
C. Ensure all persons in the data center are evacuated.
D. Remove all backups from the data center.

C is the correct answer.

Justification:

A. Life safety is always the first priority, and notifying the fire department of the alarm is not typically necessary because most data center alarms are configured to automatically report to the local authorities.
B. Fire suppression systems are designed to operate automatically, and activating the system when staff are not yet evacuated could create confusion and panic, leading to injuries or even fatalities. Manual triggering of the system could be necessary under certain conditions, but only after all other data center personnel are safely evacuated.
C. **In an emergency, safety of life is always the first priority; therefore, the complete and orderly evacuation of the facility staff would be the most important activity.**
D. Removal of backups from the data center is not an appropriate action because it could delay the evacuation of personnel. Most companies would have copies of backups in offsite storage to mitigate the risk of data loss for this type of disaster.

A4-60 An IS auditor discovers that the disaster recovery plan (DRP) for a company does not include a critical application hosted in the cloud. Management's response states that the cloud vendor is responsible for disaster recovery (DR) and DR-related testing. What is the **NEXT** course of action for the IS auditor to pursue?

A. Plan an audit of the cloud vendor.
B. Review the vendor contract to determine its DR capabilities.
C. Review an independent auditor's report of the cloud vendor.
D. Request a copy of the DRP from the cloud vendor.

B is the correct answer.

Justification:
A. Auditing the cloud vendor would be useful; however, this would only be useful if the vendor is contractually required to provide disaster recovery (DR) services.
B. DR services can only be expected from the vendor when explicitly listed in the contract with well-defined recovery time objectives and recovery point objectives. Without the contractual language, the vendor is not required to provide DR services.
C. An independent auditor's report, such as Statements on Standards for Attestation Engagements 16, on DR capabilities can be reviewed to ascertain the vendor's DR capabilities; however, this will only be fruitful if the vendor is contractually required to provide DR services.
D. A copy of DR policies can be requested to review their adequacy; however, this will only be useful if the vendor is contractually required to provide DR services.

A4-61 An IS auditor is performing a review of the disaster recovery hot site used by a financial institution. Which of the following would be the **GREATEST** concern?

A. System administrators use shared accounts which never expire at the hot site.
B. Disk space utilization data are not kept current.
C. Physical security controls at the hot site are less robust than at the main site.
D. Servers at the hot site do not have the same specifications as at the main site.

B is the correct answer.

Justification:
A. While it is not a good practice for security administrators to share accounts that do not expire, the greater risk in this scenario would be running out of disk space.
B. Not knowing how much disk space is in use and, therefore, how much is needed at the disaster recovery site could create major issues in the case of a disaster.
C. Physical security controls are important, and this would be a concern, but the more important concern would be running out of disk space. The particular physical characteristic of the disaster recovery site may call for different controls that may appear to be less robust than the main site; however, such a risk could be addressed through policy and procedures or by adding additional personnel if needed.
D. As long as the servers at the hot site are capable of running the programs that are required in a disaster recovery situation, the precise capabilities of the servers at the hot site is not a major risk. It is necessary to ensure that software configuration and settings match the servers at the main site, but it is not unusual for newer and more powerful servers to exist at the main site for everyday production use while the standby servers are less powerful.

A4-62 When reviewing system parameters, an IS auditor's **PRIMARY** concern should be that:

A. they are set to meet both security and performance requirements.
B. changes are recorded in an audit trail and periodically reviewed.
C. changes are authorized and supported by appropriate documents.
D. access to parameters in the system is restricted.

A is the correct answer.

Justification:

A. **The primary concern is to find the balance between security and performance. Recording changes in an audit trail and periodically reviewing them is a detective control; however, if parameters are not set according to business rules, monitoring of changes may not be an effective control.**
B. Reviewing changes to ensure that they are supported by appropriate documents is also a detective control.
C. If parameters are set incorrectly, the related documentation and the fact that these are authorized does not reduce the impact.
D. Restriction of access to parameters ensures that only authorized staff can access the parameters; however, if the parameters are set incorrectly, restricting access will still have an adverse impact.

A4-63 An offsite information processing facility with electrical wiring, air conditioning and flooring, but no computer or communications equipment, is a:

A. cold site.
B. warm site.
C. dial-up site.
D. duplicate processing facility.

A is the correct answer.

Justification:

A. **A cold site is ready to receive equipment but does not offer any components at the site in advance of the need.**
B. A warm site is an offsite backup facility that is partially configured with network connections and selected peripheral equipment—such as disk and tape units, controllers and central processing units—to operate an information processing facility.
C. A dial-up site is used for remote access, but not for offsite information processing.
D. A duplicate information processing facility is a dedicated, fully-developed recovery site that can back up critical applications.

A4-64 An optimized disaster recovery plan for an organization should:

A. reduce the length of the recovery time and the cost of recovery.
B. increase the length of the recovery time and the cost of recovery.
C. reduce the duration of the recovery time and increase the cost of recovery.
D. not affect the recovery time or the cost of recovery.

A is the correct answer.

Justification:

A. **One of the objectives of a disaster recovery plan (DRP) is to reduce the duration and cost of recovering from a disaster.**
B. A DRP would increase the cost of operations before and after the disaster occurs.
C. A DRP should reduce the time to return to normal operations.
D. A DRP should reduce the cost that could result from a disaster.

A4-65 A disaster recovery plan for an organization's financial system specifies that the recovery point objective is zero and the recovery time objective is 72 hours. Which of the following is the **MOST** cost-effective solution?

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

D is the correct answer.

Justification:

A. A hot site would meet the recovery time objective (RTO) but would incur higher costs than necessary.
B. Asynchronous updates of the database in distributed locations do not meet the recovery point objective (RPO).
C. Synchronous updates of the data and standby active systems in a hot site meet the RPO and RTO requirements but are costlier than a warm site solution.
D. The synchronous copy of the data storage achieves the RPO, and a warm site operational in 48 hours meets the required RTO.

A4-66 A financial institution that processes millions of transactions each day has a central communications processor (switch) for connecting to automated teller machines. Which of the following would be the **BEST** contingency plan for the communications processor?

A. Reciprocal agreement with another organization
B. Alternate processor in the same location
C. Alternate processor at another network node
D. Duplex communication links

C is the correct answer.

Justification:

A. Reciprocal agreements make an organization dependent on the other organization and raise privacy, competition and regulatory issues.
B. Having an alternate processor in the same location resolves the equipment problem but would not be effective if the failure was caused by environmental conditions (i.e., power disruption).
C. The unavailability of the central communications processor would disrupt all access to the banking network. This could be caused by an equipment, power or communications failure. Having a duplicate processor in another location that could be used for alternate processing is the best solution.
D. The installation of duplex communication links would only be appropriate if the failure were limited to the communication link.

A4-67 Which of the following provides the **BEST** evidence of an organization's disaster recovery capability readiness?

A. A disaster recovery plan (DRP)
B. Customer references for the alternate site provider
C. Processes for maintaining the DRP
D. Results of tests and exercises

D is the correct answer.

Justification:
A. Having a plan is important, but a plan cannot be considered effective until it has been tested.
B. Customer references may aid in choosing an alternate site provider but will not ensure the effectiveness of the plan.
C. A disaster recovery plan must be kept up to date through a regular maintenance and review schedule, but this is not as important as testing.
D. Only tests and exercises demonstrate the adequacy of the plans and provide reasonable assurance of an organization's disaster recovery capability readiness.

A4-68 An IS auditor finds that database administrators (DBAs) have access to the log location on the database server and the ability to purge logs from the system. What is the **BEST** audit recommendation to ensure that DBA activity is effectively monitored?

A. Change permissions to prevent DBAs from purging logs.
B. Forward database logs to a centralized log server to which the DBAs do not have access.
C. Require that critical changes to the database are formally approved.
D. Back up database logs to tape.

B is the correct answer.

Justification:
A. Changing the database administrator (DBA) permissions to prevent DBAs from purging logs may not be feasible and does not adequately protect the availability and integrity of the database logs.
B. To protect the availability and integrity of the database logs, it is most feasible to forward the database logs to a centralized log server to which the DBAs do not have access.
C. Requiring that critical changes to the database are formally approved does not adequately protect the availability and integrity of the database logs.
D. Backing up database logs to tape does not adequately protect the availability and integrity of the database logs.

A4-69 While performing a review of a critical third-party application, an IS auditor would be **MOST** concerned with discovering:

A. inadequate procedures for ensuring adequate system portability.
B. inadequate operational documentation for the system.
C. an inadequate alternate service provider listing.
D. an inadequate software escrow agreement.

D is the correct answer.

Justification:

A. Procedures to ensure that systems are developed so that they can be ported to other system platforms will help ensure that the system can still continue functioning without affecting the business process if changes to the infrastructure occur. This is less important than availability of the software.
B. Inadequate operational documentation is a risk but would be less significant than the risk of unavailability of the software.
C. While alternate service providers could be used if a vendor goes out of business, having access to the source code via a software escrow agreement is more important.
D. The inclusion of a clause in the agreement that requires software code to be placed in escrow helps to ensure that the customer can continue to use the software and/or obtain technical support if a vendor were to go out of business.

A4-70 Which of the following activities should the business continuity manager perform **FIRST** after the replacement of hardware at the primary information processing facility?

A. Verify compatibility with the hot site
B. Review the implementation report
C. Perform a walk-through of the disaster recovery plan
D. Update the IT assets inventory

D is the correct answer.

Justification:

A. Before validating that the new hardware is compatible with the recovery site, the business continuity manager should update the listing of all equipment and IT assets included in the business continuity plan.
B. The implementation report will be of limited value to the business continuity manager because the equipment has been installed.
C. The walk-through of the plan should only be done after the asset inventory has been updated.
D. An IT assets inventory is the basic input for the business continuity/disaster recovery plan, and the plan must be updated to reflect changes in the IT infrastructure.

A4-71 Which of the following would an IS auditor consider to be the **MOST** important to review when conducting a disaster recovery audit?

A. A hot site is contracted for and available as needed.
B. A business continuity manual is available and current.
C. Insurance coverage is adequate and premiums are current.
D. Data backups are performed timely and stored offsite.

D is the correct answer.

Justification:
A. A hot site is important, but it is of no use if there are no data backups for it.
B. A business continuity manual is advisable but not most important in a disaster recovery audit.
C. Insurance coverage should be adequate to cover costs but is not as important as having the data backup.
D. Without data to process, all other components of the recovery effort are in vain. Even in the absence of a plan, recovery efforts of any type would not be practical without data to process.

A4-72 Which of the following should the IS auditor review to ensure that servers are optimally configured to support processing requirements?

A. Benchmark test results
B. Server logs
C. Downtime reports
D. Server utilization data

D is the correct answer.

Justification:
A. Benchmark tests are designed to compare system performance using standardized criteria; however, benchmark testing does not provide the best data to ensure the optimal configuration of servers in an organization.
B. A server log contains data showing activities performed on the server but does not contain the utilization data required to ensure the optimal configuration of servers.
C. A downtime report identifies the elapsed time when a computer is not operating correctly because of machine failure but is not useful in determining optimal server configurations.
D. Monitoring server utilization identifies underutilized servers and monitors overall server utilization. Underutilized servers do not provide the business with optimal cost-effectiveness. By monitoring server usage, IT management can take appropriate measures to raise the utilization ratio and provide the most effective return on investment.

A4-73 Which of the following is a continuity plan test that simulates a system crash and uses actual resources to cost-effectively obtain evidence about the plan's effectiveness?

A. Paper test
B. Post-test
C. Preparedness test
D. Walk-through

C is the correct answer.

Justification:

A. A paper test is a walk-through of the plan, involving major players, who attempt to determine what might happen in a particular type of service disruption in the plan's execution. A paper test usually precedes the preparedness test.
B. A post-test is actually a test phase and is comprised of a group of activities such as returning all resources to their proper place, disconnecting equipment, returning personnel and deleting all company data from third-party systems.
C. **A preparedness test is a localized version of a full test, wherein resources are expended in the simulation of a system crash. This test is performed regularly on different aspects of the plan and can be a cost-effective way to gradually obtain evidence about the plan's effectiveness. It also provides a means to improve the plan in increments.**
D. A walk-through is a test involving a simulated disaster situation that tests the preparedness and understanding of management and staff rather than the actual resources.

A4-74 While designing the business continuity plan (BCP) for an airline reservation system, the **MOST** appropriate method of data transfer/backup at an offsite location would be:

A. shadow file processing.
B. electronic vaulting.
C. hard-disk mirroring.
D. hot-site provisioning.

A is the correct answer.

Justification:

A. **In shadow file processing, exact duplicates of the files are maintained at the same site or at a remote site. The two files are processed concurrently. This is used for critical data files such as airline booking systems.**
B. Electronic vaulting electronically transmits data either to direct access storage, an optical disc or another storage medium; this is a method used by banks. This is not usually in real time as much as a shadow file system is.
C. Hard-disk mirroring provides redundancy in case the primary hard disk fails. All transactions and operations occur on two hard disks in the same server.
D. A hot site is an alternate site ready to take over business operations within a few hours of any business interruption and is not a method for backing up data.

A4-75 Which of the following is the **BEST** method for determining the criticality of each application system in the production environment?

A. Interview the application programmers.
B. Perform a gap analysis.
C. Review the most recent application audits.
D. Perform a business impact analysis.

D is the correct answer.

Justification:
A. Interviews with the application programmers will provide limited information related to the criticality of the systems.
B. A gap analysis is relevant to system development and project management but does not determine application criticality.
C. The audits may not contain the required information about application criticality or may not have been done recently.
D. A business impact analysis (BIA) will give the impact of the loss of each application. A BIA is conducted with representatives of the business that can accurately describe the criticality of a system and its importance to the business.

A4-76 Code erroneously excluded from a production release was subsequently moved into the production environment, bypassing normal change procedures. Which of the following choices is of **MOST** concern to the IS auditor performing a post-implementation review?

A. The code was missed during the initial implementation.
B. The change did not have change management approval.
C. The error was discovered during the postimplementation review.
D. The release team used the same change order number.

B is the correct answer.

Justification:
A. Although missing a component of a release is indicative of a process deficiency, it is of more concern that the missed change was promoted into the production environment without management approval.
B. Change management approval of changes mitigates the risk of unauthorized changes being introduced to the production environment. Unauthorized changes might result in disruption of systems or fraud. It is, therefore, imperative to ensure that each change has appropriate change management approval.
C. Most release/change control errors are discovered during postimplementation review. It is of greater concern that the change was promoted without management approval after it was discovered.
D. Using the same change order number is not a relevant concern.

A4-77 A hot site should be implemented as a recovery strategy when the:

A. disaster downtime tolerance is low.
B. recovery point objective is high.
C. recovery time objective is high.
D. maximum tolerable downtime is long.

A is the correct answer.

Justification:

A. **Disaster downtime tolerance is the time gap during which the business can accept non-availability of IT facilities. If this time gap is low, recovery strategies that can be implemented within a short period of time, such as a hot site, should be used.**
B. The recovery point objective (RPO) is the earliest point in time at which it is possible to recover the data. A high RPO means that the process would result in greater losses of data.
C. A high recovery time objective means that additional time would be available for the recovery strategy, thus making other recovery alternatives—such as warm or cold sites—viable alternatives.
D. If the maximum tolerable downtime is long, then a warm or cold site is a more cost-effective solution.

A4-78 In which of the following situations is it **MOST** appropriate to implement data mirroring as the recovery strategy?

A. Disaster tolerance is high.
B. The recovery time objective is high.
C. The recovery point objective is low.
D. The recovery point objective is high.

C is the correct answer.

Justification:

A. Data mirroring is a data recovery technique, and disaster tolerance addresses the allowable time for an outage of the business.
B. The recovery time objective (RTO) is an indicator of the disaster tolerance. Data mirroring addresses data loss, not the RTO.
C. **The recovery point objective (RPO) indicates the latest point in time at which it is possible to recover the data. This determines how often the data must be backed up to minimize data loss. If the RPO is low, then the organization does not want to lose much data and must use a process such as data mirroring to prevent data loss.**
D. If the RPO is high, then a less expensive backup strategy can be used; data mirroring should not be implemented as the data recovery strategy.

A4-79 Which of the following stakeholders is the **MOST** important in terms of developing a business continuity plan?

A. Process owners
B. Application owners
C. The board of directors
D. IT management

A is the correct answer.

Justification:

A. Process owners are essential in identifying the critical business functions, recovery times and resources needed.
B. A business continuity plan (BCP) is concerned with the continuity of business processes, while applications may or may not support critical business processes.
C. The board of directors might approve the plan, but they are typically not involved in the details of developing the BCP.
D. IT management will identify the IT resources, servers and infrastructure needed to support the critical business functions as defined by the business process owners.

A4-80 Which of the following is the **MOST** efficient and sufficiently reliable way to test the design effectiveness of a change control process?

A. Test a sample population of change requests
B. Test a sample of authorized changes
C. Interview personnel in charge of the change control process
D. Perform an end-to-end walk-through of the process

D is the correct answer.

Justification:

A. Testing a sample population of changes is a test of compliance and operating effectiveness to ensure that users submitted the proper documentation/requests. It does not test the effectiveness of the design.
B. Testing changes that have been authorized may not provide sufficient assurance of the entire process because it does not test the elements of the process related to authorization or detect changes that bypassed the controls.
C. Interviewing personnel in charge of the change control process is not as effective as a walk-through of the change controls process because people may know the process but not follow it.
D. Observation is the best and most effective method to test changes to ensure that the process is effectively designed.

A4-81 During fieldwork, an IS auditor experienced a system crash caused by a security patch installation. To provide reasonable assurance that this event will not recur, the IS auditor should ensure that:

A. only systems administrators perform the patch process.
B. the client's change management process is adequate.
C. patches are validated using parallel testing in production.
D. an approval process of the patch, including a risk assessment, is developed.

B is the correct answer.

Justification:

A. While system administrators would normally install patches, it is more important that changes be made according to a formal procedure that includes testing and implementing the change during nonproduction times.
B. The change management process, which would include procedures regarding implementing changes during production hours, helps to ensure that this type of event does not recur. An IS auditor should review the change management process, including patch management procedures, to verify that the process has adequate controls and to make suggestions accordingly.
C. While patches would normally undergo testing, it is often impossible to test all patches thoroughly. It is more important that changes be made during nonproduction times, and that a backout plan is in place in case of problems.
D. An approval process alone could not directly prevent this type of incident from happening. There should be a complete change management process that includes testing, scheduling and approval.

A4-82 A batch transaction job failed in production; however, the same job returned no issues during user acceptance testing (UAT). Analysis of the production batch job indicates that it was altered after UAT. Which of the following ways would be the **BEST** to mitigate this risk in the future?

A. Improve regression test cases.
B. Activate audit trails for a limited period after release.
C. Conduct an application user access review.
D. Ensure that developers do not have access to code after testing.

D is the correct answer.

Justification:

A. Improving the quality of the testing would not be applicable in this case because the more important issue is that developers have access to the production environment.
B. Activating audit trails or performing additional logging may be useful; however, the more important issue is that developers have access to the production environment.
C. Conducting an application user access review would not identify developers' access to code because they would not be included in this review.
D. To ensure proper segregation of duties, developers should be restricted to the development environment only. If code needs to be modified after user acceptance testing, the process must be restarted in development.

A4-83 An organization completed a business impact analysis as part of business continuity planning. The **NEXT** step in the process is to develop:

A. a business continuity strategy.
B. a test and exercise plan.
C. a user training program.
D. the business continuity plan (BCP).

A is the correct answer.

Justification:

A. **A business continuity strategy is the next phase because it identifies the best way to recover. The criticality of the business process, the cost, the time required to recover, and security must be considered during this phase.**
B. The recovery strategy and plan development precede the test plan.
C. Training can only be developed once the business continuity plan (BCP) is in place.
D. A strategy must be determined before the BCP is developed.

A4-84 An IS auditor performing an application maintenance audit would review the log of program changes for the:

A. Authorization of program changes.
B. Creation date of a current object module.
C. Number of program changes actually made.
D. Creation date of a current source program.

A is the correct answer.

Justification:

A. **The auditor wants to ensure that only authorized changes have been made to the application. The auditor would therefore review the log of program changes to verify that all changes have been approved.**
B. The creation date of the current object module will not indicate earlier changes to the application.
C. The auditor will review the system to notice the number of changes actually made but then will verify that all the changes were authorized.
D. The creation date of the current source program will not identify earlier changes.

A4-85 Which of the following assures an enterprise of the existence and effectiveness of internal controls relative to the service provided by a third party?

A. The current service level agreement
B. A recent independent third-party audit report
C. The current business continuity plan procedures
D. A recent disaster recovery plan test report

B is the correct answer.

Justification:

A. A service level agreement defines the contracted level of service; however, it would not provide assurance related to internal controls.
B. **An independent third-party audit report such as a Statements on Standards for Attestation Engagements 16 would provide assurance of the existence and effectiveness of internal controls at the third party.**
C. While a business continuity plan is essential, it would not provide assurance related to internal controls.
D. While a disaster recovery plan is essential, it would not provide assurance related to internal controls.

A4-86 When reviewing a disaster recovery plan, an IS auditor should be **MOST** concerned with the lack of:

A. process owner involvement.
B. well-documented testing procedures.
C. an alternate processing facility.
D. a well-documented data classification scheme.

A is the correct answer.

Justification:

A. Process owner involvement is a critical part of the business impact analysis (BIA), which is used to create the disaster recovery plan. If the IS auditor determined that process owners were not involved, this would be a significant concern.
B. While well-documented testing procedures are important, unless process owners are involved there is no way to know whether the priorities and critical elements of the plan are valid.
C. An alternate processing facility may be a requirement to meet the needs of the business; however, such a decision needs to be based on the BIA.
D. A data classification scheme is important to ensure that controls over data are appropriate; however, this is a lesser concern than a lack of process owner involvement.

A4-87 An organization has outsourced its help desk function. Which of the following indicators would be the **BEST** to include in the service level agreement?

A. Overall number of users supported
B. First call resolution rate
C. Number of incidents reported to the help desk
D. Number of agents answering the phones

B is the correct answer.

Justification:

A. The contract price will usually be based on the number of users supported, but the performance metrics should be based on the ability to provide effective support and address user problems rapidly.
B. Because it is about service level (performance) indicators, the percentage of incidents solved on the first call is a good way to measure the effectiveness of the supporting organization.
C. The number of reported incidents cannot be controlled by the outsource supplier; therefore, that cannot be an effective measure.
D. The efficiency and effectiveness of the people answering the calls and being able to address problems rapidly are more important than the number of people answering the calls.

A4-88 Which of the following activities performed by a database administrator should be performed by a different person?

A. Deleting database activity logs
B. Implementing database optimization tools
C. Monitoring database usage
D. Defining backup and recovery procedures

A is the correct answer.

Justification:

A. **Because database activity logs record activities performed by the database administrator (DBA), deleting them should be performed by an individual other than the DBA. This is a compensating control to aid in ensuring an appropriate segregation of duties and is associated with the DBA's role.**
B. Implementing database optimization tools is part of the DBA's normal job function.
C. Monitoring database usage is part of the DBA's normal job function.
D. Defining backup and recovery procedures is part of the DBA's normal job function.

A4-89 Which of the following is the **BEST** reason for integrating the testing of non-critical systems in disaster recovery plans (DRPs) with business continuity plans (BCPs)?

A. To ensure that DRPs are aligned to the business impact analysis.
B. Infrastructure recovery personnel can be assisted by business subject matter experts.
C. BCPs may assume the existence of capabilities that are not in DRPs.
D. To provide business executives with knowledge of disaster recovery capabilities.

C is the correct answer.

Justification:

A. Disaster recovery plans (DRPs) should be aligned with the business impact analysis; however, this has no impact on integrating the testing of noncritical systems in DRPs with business continuity plans (BCPs).
B. Infrastructure personnel will be focused on restoring the various platforms that make up the infrastructure, and it is not necessary for business subject matter experts to be involved.
C. **BCPs may assume the existence of capabilities that are not part of the DRPs, such as allowing employees to work from home during the disaster; however, IT may not have made sufficient provisions for these capabilities (e.g., they cannot support a large number of employees working from home). While the noncritical systems are important, it is possible that they are not part of the DRPs. For example, an organization may use an online system that does not interface with the internal systems. If the business function using the system is a critical process, the system should be tested, and it may not be part of the DRP. Therefore, DRP and BCP testing should be integrated.**
D. While business executives may be interested in the benefits of disaster recovery, testing is not the best way to accomplish this task.

A4-90 An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions.
B. Implement before-and-after image reporting.
C. Use tracing and tagging.
D. Implement integrity constraints in the database.

D is the correct answer.

Justification:
A. Logging all table update transactions is a detective control that would not help avoid invalid data entry.
B. Implementing before-and-after image reporting is a detective control that would not help avoid the situation.
C. Tracing and tagging are used to test application systems and controls and could not prevent out-of-range data.
D. Implementing integrity constraints in the database is a preventive control because data are checked against predefined tables or rules, preventing any undefined data from being entered.

A4-91 An IS auditor discovers that some users have installed personal software on their PCs. This is not explicitly forbidden by the security policy. Of the following, the **BEST** approach for an IS auditor is to recommend that the:

A. IT department implement control mechanisms to prevent unauthorized software installation.
B. Security policy be updated to include the specific language regarding unauthorized software.
C. IT department prohibit the download of unauthorized software.
D. Users obtain approval from an IS manager before installing nonstandard software.

B is the correct answer.

Justification:
A. An IS auditor's obligation is to report on observations noted and make the best recommendation, which is to address the situation through policy. The IT department cannot implement controls in the absence of the authority provided through policy.
B. Lack of specific language addressing unauthorized software in the acceptable use policy is a weakness in administrative controls. The policy should be reviewed and updated to address the issue—and provide authority for the IT department to implement technical controls.
C. Preventing downloads of unauthorized software is not the complete solution. Unauthorized software can be also introduced through compact discs (CDs) and universal serial bus (USB) drives.
D. Requiring approval from the IS manager before installation of the nonstandard software is an exception handling control. It would not be effective unless a preventive control to prohibit user installation of unauthorized software is established first.

A4-92 The purpose of code signing is to provide assurance that:

A. the software has not been subsequently modified.
B. the application can safely interface with another signed application.
C. the signer of the application is trusted.
D. the private key of the signer has not been compromised.

A is the correct answer.

Justification:

A. Code signing ensures that the executable code came from a reputable source and has not been modified after being signed.
B. The signing of code will not ensure that it will integrate with other applications.
C. Code signing will provide assurance of the source but will not ensure that the source is trusted. The code signing will, however, ensure that the code has not been modified.
D. The compromise of the sender's private key would result in a loss of trust and is not the purpose of code signing.

A4-93 An IS auditor analyzing the audit log of a database management system (DBMS) finds that some transactions were partially executed as a result of an error and have not been rolled back. Which of the following transaction processing features has been violated?

A. Consistency
B. Isolation
C. Durability
D. Atomicity

D is the correct answer.

Justification:

A. Consistency ensures that the database is in a proper state when the transaction begins and ends and that the transaction has not violated integrity rules.
B. Isolation means that, while in an intermediate state, the transaction data are invisible to external operations. This prevents two transactions from attempting to access the same data at the same time.
C. Durability guarantees that a successful transaction will persist and cannot be undone.
D. Atomicity guarantees that either the entire transaction is processed or none of it is.

A4-94 Responsibility and reporting lines cannot always be established when auditing automated systems because:

A. diversified control makes ownership irrelevant.
B. staff traditionally changes jobs with greater frequency.
C. ownership is difficult to establish where resources are shared.
D. duties change frequently in the rapid development of technology.

C is the correct answer.

Justification:

A. Ownership is required to ensure that someone has responsibility for the secure and proper operation of a system and the protection of data.
B. The movement of staff is not a serious issue because the responsibility should be linked to a job description, not an individual.
C. The actual data and/or application owner may be hard to establish because of the complex nature of both data and application systems and many systems support more than one business department.
D. Duties may change frequently, but that does not absolve the organization of having a declared owner for systems and data.

A4-95 Which of the following distinguishes a business impact analysis from a risk assessment?

A. An inventory of critical assets
B. An identification of vulnerabilities
C. A listing of threats
D. A determination of acceptable downtime

D is the correct answer.

Justification:
A. An inventory of critical assets is completed in both a risk assessment and a business impact analysis (BIA).
B. An identification of vulnerabilities is relevant in both a risk assessment and a BIA.
C. A listing of threats is relevant both in a risk assessment and a BIA.
D. A determination of acceptable downtime is made only in a BIA.

A4-96 When reviewing a hardware maintenance program, an IS auditor should assess whether:

A. the schedule of all unplanned maintenance is maintained.
B. it is in line with historical trends.
C. it has been approved by the IS steering committee.
D. the program is validated against vendor specifications.

D is the correct answer.

Justification:
A. Unplanned maintenance cannot be scheduled.
B. Hardware maintenance programs do not necessarily need to be in line with historic trends.
C. Maintenance schedules normally are not approved by the steering committee.
D. Although maintenance requirements vary based on complexity and performance workloads, a hardware maintenance schedule should be validated against the vendor-provided specifications.

A4-97 An IS auditor should recommend the use of library control software to provide reasonable assurance that:

A. program changes have been authorized.
B. only thoroughly tested programs are released.
C. modified programs are automatically moved to production.
D. source and executable code integrity is maintained.

A is the correct answer.

Justification:
A. Library control software should be used to separate test from production libraries in mainframe and/or client server environments. The main objective of library control software is to provide assurance that program changes have been authorized.
B. Library control software is concerned with authorized program changes and cannot determine whether programs have been thoroughly tested.
C. Programs should not be moved automatically into production without proper authorization.
D. Library control software provides reasonable assurance that the source code and executable code are matched at the time a source code is moved to production. Access control will ensure the integrity of the software, but the most important benefit of version control software is to ensure that all changes are authorized.

A4-98 Which of the following would help to ensure the portability of an application connected to a database?

A. Verification of database import and export procedures
B. Usage of a Structured Query Language
C. Analysis of stored procedures/triggers
D. Synchronization of the entity-relation model with the database physical schema

B is the correct answer.

Justification:
A. Verification of import and export procedures with other systems ensures better interfacing with other systems but does not contribute to the portability of an application connecting to a database.
B. The use of Structured Query Language facilitates portability because it is an industry standard used by many systems.
C. Analyzing stored procedures/triggers ensures proper access/performance but does not contribute to the portability of an application connecting to a database.
D. Reviewing the design entity-relation model will be helpful but does not contribute to the portability of an application connecting to a database.

A4-99 Business units are concerned about the performance of a newly implemented system. Which of the following should an IS auditor recommend?

A. Develop a baseline and monitor system usage.
B. Define alternate processing procedures.
C. Prepare the maintenance manual.
D. Implement the changes users have suggested.

A is the correct answer.

Justification:
A. An IS auditor should recommend the development of a performance baseline and monitor the system's performance against the baseline to develop empirical data upon which decisions for modifying the system can be made.
B. Alternate processing procedures will not alter a system's performance, and no changes should be made until the reported issue has been examined more thoroughly.
C. A maintenance manual will not alter a system's performance or address the user concerns.
D. Implementing changes without knowledge of the cause(s) for the perceived poor performance may not result in a more efficient system.

A4-100 The **PRIMARY** objective of service-level management is to:

A. define, agree on, record and manage the required levels of service.
B. ensure that services are managed to deliver the highest achievable level of availability.
C. keep the costs associated with any service at a minimum.
D. monitor and report any legal noncompliance to business management.

A is the correct answer.

Justification:
A. The objective of service-level management (SLM) is to negotiate, document and manage (i.e., provide and monitor) the services in the manner in which the customer requires those services.
B. SLM does not necessarily ensure that services are delivered at the highest achievable level of availability (e.g., redundancy and clustering). Although maximizing availability might be necessary for some critical services, it cannot be applied as a general rule of thumb.
C. SLM cannot ensure that costs for all services will be kept at a low or minimum level because costs associated with a service will directly reflect the customer's requirements.
D. Monitoring and reporting legal noncompliance is not a primary objective of SLM.

A4-101 Which of the following should be a **MAJOR** concern for an IS auditor reviewing a business continuity plan?

A. The plan is approved by the chief information officer.
B. The plan contact lists have not been updated.
C. Test results are not adequately documented.
D. The training schedule for recovery personnel is not included.

C is the correct answer.

Justification:

A. Ideally, the board of directors should approve the plan to ensure acceptability, but it is possible to delegate approval authority to the chief information officer. Pragmatically, lack of documenting test results could have more significant consequences.
B. The contact lists are an important part of the business continuity plan (BCP); however, they are not as important as documenting the test results.
C. The effectiveness of a BCP can best be determined through tests. If results of tests are not documented, then there is no basis for feedback, updates, etc.
D. If test results are documented, a need for training will be identified and the BCP will be updated.

A4-102 Which of the following processes will be **MOST** effective in reducing the risk that unauthorized software on a backup server is distributed to the production server?

A. Manually copy files to accomplish replication.
B. Review changes in the software version control system.
C. Ensure that developers do not have access to the backup server.
D. Review the access control log of the backup server.

B is the correct answer.

Justification:

A. Even if replication is be conducted manually with due care, there still remains a risk to copying unauthorized software from one server to another.
B. It is common practice for software changes to be tracked and controlled using version control software. An IS auditor should review reports or logs from this system to identify the software that is promoted to production. Only moving the versions on the version control system program will prevent the transfer of development or earlier versions.
C. If unauthorized code was introduced onto the backup server by developers, controls on the production server and the software version control system should mitigate this risk.
D. Review of the access log will identify staff access or the operations performed; however, it may not provide enough information to detect the release of unauthorized software.

A4-103 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:

A. apply the patch according to the patch's release notes.
B. ensure that a good change management process is in place.
C. thoroughly test the patch before sending it to production.
D. approve the patch after doing a risk assessment.

B is the correct answer.

Justification:
A. The IS auditor should not apply the patch. That is an administrator responsibility.
B. An IS auditor must review the change management process, including patch management procedures, and verify that the process has adequate controls and make suggestions accordingly.
C. The testing of the patch is the responsibility of the development or production support team, not the auditor.
D. The IS auditor is not authorized to approve a patch. That is a responsibility of a steering committee.

A4-104 During maintenance of a relational database, several values of the foreign key in a transaction table have been corrupted. The consequence is that:

A. the detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
B. there is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
C. the database will immediately stop execution and lose more information.
D. the database will no longer accept input data.

A is the correct answer.

Justification:
A. When the external key of a transaction is corrupted or lost, the application system will normally be incapable of directly attaching the master data to the transaction data. Normally, this will cause the system to undertake a sequential search and slow down the processing. If the concerned files are big, this slowdown will be unacceptable. This is a violation of referential integrity.
B. A system can recover the corrupted external key by re-indexing the table.
C. The corruption of a foreign key will not stop program execution.
D. The corruption of a foreign key will not affect database input.

A4-105 In a relational database with referential integrity, the use of which of the following keys would prevent deletion of a row from a customer table as long as the customer number of that row is stored with live orders on the orders table?

A. Foreign key
B. Primary key
C. Secondary key
D. Public key

A is the correct answer.

Justification:

A. **In a relational database with referential integrity, the use of foreign keys would prevent events such as primary key changes and record deletions, resulting in orphaned relations within the database.**
B. It should not be possible to delete a row from a customer table when the customer number (primary key) of that row is stored with live orders on the orders table (the foreign key to the customer table). A primary key works in one table so it is not able to provide/ensure referential integrity by itself.
C. Secondary keys that are not foreign keys are not subject to referential integrity checks.
D. A public key is related to encryption and not linked in any way to referential integrity.

A4-106 The **PRIMARY** objective of testing a business continuity plan is to:

A. familiarize employees with the business continuity plan.
B. ensure that all residual risk is addressed.
C. exercise all possible disaster scenarios.
D. identify limitations of the business continuity plan.

D is the correct answer.

Justification:

A. Familiarizing employees with the business continuity plan is a secondary benefit of a test.
B. It is not cost-effective to address all residual risk in a business continuity plan.
C. It is not practical to test all possible disaster scenarios.
D. **Testing the business continuity plan provides the best evidence of any limitations that may exist.**

A4-107 An IS auditor examining the security configuration of an operating system should review the:

A. transaction logs.
B. authorization tables.
C. parameter settings.
D. routing tables.

C is the correct answer.

Justification:

A. Transaction logs are used to track and analyze transactions related to an application or system interface, but that is not the primary source of audit evidence in an operating system audit.
B. Authorization tables are used to verify implementation of logical access controls and will not be of much help when reviewing control features of an operating system.
C. **Configuration parameters allow a standard piece of software to be customized for diverse environments and are important in determining how a system runs. The parameter settings should be appropriate to an organization's workload and control environment. Improper implementation and/or monitoring of operating systems can result in undetected errors and corruption of the data being processed, as well as lead to unauthorized access and inaccurate logging of system usage.**
D. Routing tables do not contain information about the operating system and, therefore, provide no information to aid in the evaluation of controls.

A4-108 During a data center audit, an IS auditor observes that some parameters in the tape management system are set to bypass or ignore tape header records. Which of the following is the **MOST** effective compensating control for this weakness?

A. Staging and job setup
B. Supervisory review of logs
C. Regular backup of tapes
D. Offsite storage of tapes

A is the correct answer.

Justification:

A. **If the IS auditor finds that there are effective staging and job setup processes, this can be accepted as a compensating control. Not reading header records may otherwise result in loading the wrong tape and deleting or accessing data on the loaded tape.**
B. Supervisory review of logs is a detective control that would not prevent loading of the wrong tapes.
C. Regular tape backup is not related to bypassing tape header records.
D. Offsite storage of tapes would not prevent loading the wrong tape because of bypassing header records.

A4-109 While reviewing the IT infrastructure, an IS auditor notices that storage resources are continuously being added. The IS auditor should:

A. recommend the use of disk mirroring.
B. review the adequacy of offsite storage.
C. review the capacity management process.
D. recommend the use of a compression algorithm.

C is the correct answer.

Justification:

A. A disk mirroring solution would increase storage requirements. This would not be advisable until a proper capacity management plan is in place.
B. Offsite storage is unrelated to the problem.
C. **Capacity management is the planning and monitoring of computer resources to ensure that available IT resources are used efficiently and effectively. This will look at capacity from a strategic viewpoint and allow a plan to forecast and purchase additional equipment in a planned manner.**
D. Though data compression may save disk space, it could affect system performance. This is not the first choice—the auditor should recommend more investigation into the increased demand for storage before providing any recommended solutions.

A4-110 Which of the following is the **GREATEST** risk of an organization using reciprocal agreements for disaster recovery between two business units?

A. The documents contain legal deficiencies.
B. Both entities are vulnerable to the same incident.
C. IT systems are not identical.
D. One party has more frequent disruptions than the other.

B is the correct answer.

Justification:

A. Inadequate agreements between two business units is a risk, but generally a lesser one than the risk that both organizations will suffer a disaster at the same time.
B. **The use of reciprocal disaster recovery is based on the probability that both organizations will not suffer a disaster at the same time.**
C. While incompatible IT systems could create problems, it is a less significant risk than both organizations suffering from the same disaster at the same time.
D. While one party may use the other's resources more frequently, this can be addressed by contractual provisions and is not a major risk.

A4-111 In determining the acceptable time period for the resumption of critical business processes:

A. only downtime costs need to be considered.
B. recovery operations should be analyzed.
C. both downtime costs and recovery costs need to be evaluated.
D. indirect downtime costs should be ignored.

C is the correct answer.

Justification:

A. Downtime costs cannot be looked at in isolation. The quicker information assets can be restored and business processing resumed, the smaller the downtime costs. However, the expenditure needed to have the redundant capability required to rapidly recover information resources might be prohibitive for nonessential business processes.
B. Recovery operations alone do not determine the acceptable time period for the resumption of critical business processes, and indirect downtime costs should be considered in addition to the direct cash outflows incurred due to business disruption.
C. **Both downtime costs and recovery costs need to be evaluated in determining the acceptable time period before the resumption of critical business processes. The outcome of the business impact analysis should be a recovery strategy that represents the optimal balance.**
D. The indirect costs of a serious disruption to normal business activity (e.g., loss of customer and supplier goodwill and loss of market share) may actually be more significant than direct costs over time, thus reaching the point where business viability is threatened.

A4-112 To verify that the correct version of a data file was used for a production run, an IS auditor should review:

A. operator problem reports.
B. operator work schedules.
C. system logs.
D. output distribution reports.

C is the correct answer.

Justification:

A. Operator problem reports are used by operators to log computer operation problems.
B. Operator work schedules are maintained to assist in human resource planning.
C. **System logs are automated reports which identify most of the activities performed on the computer. Programs that analyze the system log have been developed to report on specifically defined items. The IS auditor can then carry out tests to ensure that the correct file version was used for a production run.**
D. Output distribution reports identify all application reports generated and their distribution.

A4-113 The **BEST** audit procedure to determine if unauthorized changes have been made to production code is to:

A. examine the change control system records and trace them forward to object code files.
B. review access control permissions operating within the production program libraries.
C. examine object code to find instances of changes and trace them back to change control records.
D. review change approved designations established within the change control system.

C is the correct answer.

Justification:
A. Checking the change control system will not detect changes that were not recorded in the control system.
B. Reviewing access control permissions will not identify unauthorized changes made previously.
C. The procedure of examining object code files to establish instances of code changes and tracing these back to change control system records is a substantive test that directly addresses the risk of unauthorized code changes.
D. Reviewing change approved designations will not identify unauthorized changes.

A4-114 When performing a database review, an IS auditor notices that some tables in the database are not normalized. The IS auditor should next:

A. recommend that the database be normalized.
B. review the conceptual data model.
C. review the stored procedures.
D. review the justification.

D is the correct answer.

Justification:
A. The IS auditor should not recommend normalizing the database until further investigation takes place.
B. Reviewing the conceptual data model will not provide information about normalization or the justification for the level of normalization.
C. Reviewing the stored procedures will not provide information about normalization.
D. If the database is not normalized, the IS auditor should review the justification because, in some situations, denormalization is recommended for performance reasons.

A4-115 Which of the following would be **MOST** important for an IS auditor to verify while conducting a business continuity audit?

A. Data backups are performed on a timely basis.
B. A recovery site is contracted for and available as needed.
C. Human safety procedures are in place.
D. Insurance coverage is adequate and premiums are current.

C is the correct answer.

Justification:
A. Performing data backups is necessary for a business continuity plan, but the IS auditor will always be most concerned with human safety.
B. A recovery site is important for business continuity, but life safety is always the first priority.
C. The most important element in any business continuity process is the protection of human life. This takes precedence over all other aspects of the plan.
D. Insurance coverage is not as important as life safety.

A4-116 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?

A. Rewrite the patches and apply them.
B. Review the code and application of available patches.
C. Develop in-house patches.
D. Identify and test suitable patches before applying them.

D is the correct answer.

Justification:
A. Rewriting the patches and applying them would require skilled resources and time to rewrite the patches.
B. Code review could be possible, but tests need to be performed before applying the patches.
C. Because the system was developed outside the organization, the IT department may not have the necessary skills and resources to develop patches.
D. Suitable patches from the existing developers should be selected and tested before applying them.

A4-117 During the audit of a database server, which of the following would be considered the **GREATEST** exposure?

A. The password on the administrator account does not expire.
B. Default global security settings for the database remain unchanged.
C. Old data have not been purged.
D. Database activity is not fully logged.

B is the correct answer.

Justification:
A. A nonexpiring password is a risk and an exposure but not as serious a risk as a weak password or the continued use of default settings.
B. Default security settings for the database could allow issues such as blank user passwords or passwords that were the same as the username.
C. Failure to purge old data may present a performance issue but is not an immediate security concern.
D. Logging all database activity is a potential risk but not as serious a risk as default settings.

A4-118 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?

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

B is the correct answer.

Justification:
A. Having a log is not a control; reviewing the log is a control.
B. The matching of hash keys over time would allow detection of changes to files.
C. Because the access was already granted at the command line level, it will be possible for the developers to bypass the control.
D. Removing the tools from the production environment will not mitigate the risk of unauthorized activity by the developers.

A4-119 A new application has been purchased from a vendor and is about to be implemented. Which of the following choices is a key consideration when implementing the application?

A. Preventing the compromise of the source code during the implementation process
B. Ensuring that vendor default accounts and passwords have been disabled
C. Removing the old copies of the program from escrow to avoid confusion
D. Verifying that the vendor is meeting support and maintenance agreements

B is the correct answer.

Justification:
A. The source code may not even be available to the purchasing organization, and it is the executable or object code that must be protected during implementation.
B. Disabling vendor default accounts and passwords is a critical part of implementing a new application.
C. Because this is a new application, there should not be any problem with older versions in escrow.
D. It is not possible to ensure that the vendor is meeting support and maintenance requirements until the system is operating.

A4-120 The **MAIN** criterion for determining the severity level of a service disruption incident is:

A. cost of recovery.
B. negative public opinion.
C. geographic location.
D. downtime.

D is the correct answer.

Justification:
A. The cost of recovery could be minimal, yet the service downtime could have a major impact.
B. Negative public opinion is a symptom of an incident; it is a factor in determining impact but not the most important one.
C. Geographic location does not determine the severity of the incident.
D. The longer the period of time a client cannot be serviced, the greater the severity (impact) of the incident.

A4-121 Doing which of the following during peak production hours could result in unexpected downtime?

A. Performing data migration or tape backup
B. Performing preventive maintenance on electrical systems
C. Promoting applications from development to the staging environment
D. Reconfiguring a standby router in the data center

B is the correct answer.

Justification:
A. Performing data migration may impact performance but would not cause downtime.
B. Preventive maintenance activities should be scheduled for non-peak times of the day, and preferably during a maintenance window time period. A mishap or incident caused by a maintenance worker could result in unplanned downtime.
C. Promoting applications into a staging environment (not production) should not affect systems operations in any significant manner.
D. Reconfiguring a standby router should not cause unexpected downtime because the router is not operational and any problems should not affect network traffic.

A4-122 During a human resources (HR) audit, an IS auditor is informed that there is a verbal agreement between the IT and HR departments as to the level of IT services expected. In this situation, what should the IS auditor do **FIRST**?

A. Postpone the audit until the agreement is documented.
B. Report the existence of the undocumented agreement to senior management.
C. Confirm the content of the agreement with both departments.
D. Draft a service level agreement for the two departments.

C is the correct answer.

Justification:

A. There is no reason to postpone an audit because a service agreement is not documented, unless that is all that is being audited. The agreement can be documented after it has been established that there is an agreement in place.
B. Reporting to senior management is not necessary at this stage of the audit because this is not a serious immediate vulnerability.
C. An IS auditor should first confirm and understand the current practice before making any recommendations. Part of this will be to ensure that both parties agree with the terms of the agreement.
D. Drafting a service level agreement is not the IS auditor's responsibility.

A4-123 A database administrator has detected a performance problem with some tables, which could be solved through denormalization. This situation will increase the risk of:

A. concurrent access.
B. deadlocks.
C. unauthorized access to data.
D. a loss of data integrity.

D is the correct answer.

Justification:

A. Denormalization will have no effect on concurrent access to data in a database; concurrent access is resolved through locking.
B. Deadlocks are a result of locking of records. This is not related to normalization.
C. Access to data is controlled by defining user rights to information and is not affected by denormalization.
D. Normalization is the removal of redundant data elements from the database structure. Disabling normalization in relational databases will create redundancy and a risk of not maintaining consistency of data, with the consequent loss of data integrity.

A4-124 Which of the following processes should an IS auditor recommend to assist in the recording of baselines for software releases?

A. Change management
B. Backup and recovery
C. Incident management
D. Configuration management

D is the correct answer.

Justification:
A. Change management is important to control changes to the configuration, but the baseline itself refers to a standard configuration.
B. Backup and recovery of the configuration are important, but not used to create the baseline.
C. Incident management will determine how to respond to an adverse event but is not related to recording baseline configurations.
D. The configuration management process may include automated tools that will provide an automated recording of software release baselines. Should the new release fail, the baseline will provide a point to which to return.

A4-125 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 that IT has **NOT** considered:

A. the training needs for users after applying the patch.
B. any beneficial impact of the patch on the operational systems.
C. delaying deployment until testing the impact of the patch.
D. the necessity of advising end users of new patches.

C is the correct answer.

Justification:
A. Normally, there is no need for training users when a new operating system patch has been installed.
B. Any beneficial impact is less important than the risk of unavailability, which could be avoided with proper testing.
C. Deploying patches without testing exposes an organization to the risk of system disruption or failure.
D. Normally, there is no need for advising users when a new operating system patch has been installed except to ensure that the patch is applied at a time that will have minimal impact on operations.

A4-126 The **BEST** method for assessing the effectiveness of a business continuity plan is to review the:

A. plans and compare them to appropriate standards.
B. results from previous tests.
C. emergency procedures and employee training.
D. offsite storage and environmental controls.

B is the correct answer.

Justification:
A. Comparisons to standards will give some assurance that the plan addresses the critical aspects of a business continuity plan but will not reveal anything about its effectiveness.
B. Previous test results will provide evidence of the effectiveness of the business continuity plan.
C. Reviewing emergency procedures would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.
D. Reviewing offsite storage and environmental controls would provide insight into some aspects of the plan but would fall short of providing assurance of the plan's overall effectiveness.

A4-127 With respect to business continuity strategies, an IS auditor interviews key stakeholders in an organization to determine whether they understand their roles and responsibilities. The IS auditor is attempting to evaluate the:

A. clarity and simplicity of the business continuity plans.
B. adequacy of the business continuity plans.
C. effectiveness of the business continuity plans.
D. ability of IS and end-user personnel to respond effectively in emergencies.

A is the correct answer.

Justification:

A. **The IS auditor should interview key stakeholders to evaluate how well they understand their roles and responsibilities. When all stakeholders have a detailed understanding of their roles and responsibilities in the event of a disaster, an IS auditor can deem the business continuity plan to be clear and simple.**
B. To evaluate adequacy, the IS auditor should review the plans and compare them to appropriate standards and the results of tests of the plan.
C. To evaluate effectiveness, the IS auditor should review the results from previous tests or incidents. This is the best determination for the evaluation of effectiveness. An understanding of roles and responsibilities by key stakeholders will assist in ensuring the business continuity plan is effective.
D. To evaluate the response, the IS auditor should review results of continuity tests. This will provide the IS auditor with assurance that target and recovery times are met. Emergency procedures and employee training need to be reviewed to determine whether the organization has implemented plans to allow for an effective response.

A4-128 During the design of a business continuity plan, the business impact analysis identifies critical processes and supporting applications. This will **PRIMARILY** influence the:

A. responsibility for maintaining the business continuity plan.
B. criteria for selecting a recovery site provider.
C. recovery strategy.
D. responsibilities of key personnel.

C is the correct answer.

Justification:

A. The responsibility for maintaining the business continuity plan is decided after the selection or design of the appropriate recovery strategy and development of the plan.
B. The criteria for selecting a recovery site provider are decided after the selection or design of the appropriate recovery strategy.
C. **The most appropriate strategy is selected based on the relative risk level, time lines and criticality identified in the business impact analysis.**
D. The responsibilities of key personnel are decided after the selection or design of the appropriate recovery strategy during the plan development phase.

A4-129 During a review of a business continuity plan, an IS auditor noticed that the point at which a situation is declared to be a crisis has not been defined. The **MAJOR** risk associated with this is that:

A. assessment of the situation may be delayed.
B. execution of the disaster recovery plan could be impacted.
C. notification of the teams might not occur.
D. potential crisis recognition might be delayed.

B is the correct answer.

Justification:

A. Problem and severity assessment would provide information necessary in declaring a disaster, but the lack of a crisis declaration point would not delay the assessment.
B. Execution of the business continuity and disaster recovery plans would be impacted if the organization does not know when to declare a crisis.
C. After a potential crisis is recognized, the teams responsible for crisis management need to be notified. Delaying the declaration of a disaster would impact or negate the effect of having response teams, but this is only one part of the larger impact.
D. Potential crisis recognition is the first step in recognizing or responding to a disaster and would occur prior to the declaration of a disaster.

A4-130 An organization has just completed its annual risk assessment. Regarding the business continuity plan, what should an IS auditor recommend as the next step for the organization?

A. Review and evaluate the business continuity plan for adequacy
B. Perform a full simulation of the business continuity plan
C. Train and educate employees regarding the business continuity plan
D. Notify critical contacts in the business continuity plan

A is the correct answer.

Justification:

A. The business continuity plan should be reviewed every time a risk assessment is completed for the organization.
B. Performing a simulation should be completed after the business continuity plan has been deemed adequate for the organization.
C. Training of the employees should be performed after the business continuity plan has been deemed adequate for the organization.
D. There is no reason to notify the business continuity plan contacts at this time.

A4-131 Which of the following database controls would ensure that the integrity of transactions is maintained in an online transaction processing system's database?

A. Authentication controls
B. Data normalization controls
C. Read/write access log controls
D. Commitment and rollback controls

D is the correct answer.

Justification:

A. Authentication controls would ensure that only authorized personnel can make changes but would not ensure the integrity of the changes.
B. Data normalization is not used to protect the integrity of online transactions.
C. Log controls are a detective control but will not ensure the integrity of the data in the database.
D. Commitment and rollback controls are directly relevant to integrity. These controls ensure that database operations that form a logical transaction unit will be completed entirely or not at all (i.e., if, for some reason, a transaction cannot be fully completed, then incomplete inserts/updates/deletes are rolled back so that the database returns to its pretransition state).

A4-132 An IS auditor finds that the data warehouse query performance decreases significantly at certain times of the day. Which of the following controls would be **MOST** relevant for the IS auditor to review?

A. Permanent table-space allocation
B. Commitment and rollback controls
C. User spool and database limit controls
D. Read/write access log controls

C is the correct answer.

Justification:

A. Table-space allocation will not affect performance at different times of the day.
B. Commitment and rollback will only apply to errors or failures and will not affect performance at different times of the day.
C. User spool limits restrict the space available for running user queries. This prevents poorly formed queries from consuming excessive system resources and impacting general query performance. Limiting the space available to users in their own databases prevents them from building excessively large tables. This helps to control space utilization which itself acts to help performance by maintaining a buffer between the actual data volume stored and the physical device capacity. Additionally, it prevents users from consuming excessive resources in ad hoc table builds (as opposed to scheduled production loads that often can run overnight and are optimized for performance purposes). In a data warehouse, because you are not running online transactions, commitment and rollback does not have an impact on performance.
D. Read/write access log controls will not affect performance at different times of the day.

A4-133 In a small organization, developers may release emergency changes directly to production. Which of the following will **BEST** control the risk in this situation?

A. Approve and document the change the next business day.
B. Limit developer access to production to a specific time frame.
C. Obtain secondary approval before releasing to production.
D. Disable the compiler option in the production machine.

A is the correct answer.

Justification:
A. It may be appropriate to allow programmers to make emergency changes as long as they are documented and approved after the fact.
B. Restricting release time frame may help somewhat; however, it would not apply to emergency changes and cannot prevent unauthorized release of the programs.
C. Obtaining secondary approval before releasing to production is not relevant in an emergency situation.
D. Disabling the compiler option in the production machine is not relevant in an emergency situation.

A4-134 Of the following alternatives, the **FIRST** approach to developing a disaster recovery strategy would be to assess whether:

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

B is the correct answer.

Justification:
A. It is impossible to remove all existing and future threats.
B. It is critical to initially identify information assets that can be made more resilient to disasters (e.g., diverse routing, alternate paths or multiple communication carriers). Preventing a problem is always better than planning to address a problem when it happens.
C. The optimization of the recovery time objective comes later in the development of the disaster recovery strategy.
D. Efforts to minimize the cost of recovery come later in the development of the disaster recovery strategy.

A4-135 An IS auditor determined that the IT manager recently changed the vendor that is responsible for performing maintenance on critical computer systems to cut costs. While the new vendor is less expensive, the new maintenance contract specifies a change in incident resolution time specified by the original vendor. Which of the following should be the **GREATEST** concern to the IS auditor?

A. Disaster recovery plans may be invalid and need to be revised.
B. Transactional business data may be lost in the event of system failure.
C. The new maintenance vendor is not familiar with the organization's policies.
D. Application owners were not informed of the change.

D is the correct answer.

Justification:

A. Disaster recovery plans (DRPs) must support the needs of the business, but the greater risk is that application owners are not aware of the change in resolution time.
B. Transactional business data loss is determined by data backup frequency and, consequently, the backup schedule.
C. The vendor must abide by the terms of the contract and those should include compliance with the privacy policies of the organization, but the lack of application owner involvement is the most important concern.
D. The greatest risk of making a change to the maintenance of critical systems is that the change could have an adverse impact on a critical business process. While there is a benefit in selecting a less expensive maintenance vendor, the resolution time must be aligned with the needs of the business.

A4-136 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?

A. Daily data backup to tape and storage at a remote site
B. Real-time replication to a remote site
C. Hard disk mirroring to a local server
D. Real-time data backup to the local storage area network

B is the correct answer.

Justification:

A. Daily tape backup recovery could result in a loss of a day's work of data.
B. With real-time replication to a remote site, data are updated simultaneously in two separate locations; therefore, a disaster in one site would not damage the information located in the remote site. This assumes that both sites were not affected by the same disaster.
C. Hard disk mirroring to a local server takes place in the same data center and could possibly be affected by the same disaster.
D. Real-time data backup to the local storage area network takes place in the same data center and could possibly be affected by the same disaster.

A4-137 If the recovery time objective increases:

A. the disaster tolerance increases.
B. the cost of recovery increases.
C. a cold site cannot be used.
D. the data backup frequency increases.

A is the correct answer.

Justification:

A. **The longer the recovery time objective (RTO), the higher disaster tolerance. The disaster tolerance is the amount of time the business can afford to be disrupted before resuming critical operations.**
B. The longer the RTO, the lower the recovery cost.
C. It cannot be concluded that a cold site is inappropriate; with a longer RTO the use of a cold site may become feasible.
D. RTO is not related to the frequency of data backups—that is related to recovery point objective.

A4-138 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?

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

A is the correct answer.

Justification:

A. **If a new disaster recovery plan (DRP) is not tested, the possibility of a catastrophic service interruption that the organization cannot recover from is the most critical of all risk.**
B. A DRP that has not been tested may lead to a higher consumption of resources than expected, but that is not the most critical risk.
C. An untested DRP may be inefficient and lead to extraordinary costs, but the most serious risk is the failure of critical services.
D. Testing educates users and recovery teams so that they can effectively execute the DRP, but the most critical risk is the failure of core business services.

A4-139 When developing a disaster recovery plan, the criteria for determining the acceptable downtime should be the:

A. annual loss expectancy.
B. service delivery objective.
C. quantity of orphan data.
D. maximum tolerable outage.

D is the correct answer.

Justification:

A. The acceptable downtime would not be determined by the annual loss expectancy (ALE); ALE is related to risk management calculations, not disaster recovery.
B. The service delivery objective is relevant to business continuity, but it is not determined by acceptable downtime.
C. The quantity of orphan data is relevant to business continuity, but it is not determined by acceptable downtime.
D. 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.

A4-140 During the review of an enterprise's preventive maintenance process for systems at a data center, the IS auditor has determined that adequate maintenance is being performed on all critical computing, power and cooling systems. Additionally, it is **MOST** important for the IS auditor to ensure that the organization:

A. has performed background checks on all service personnel.
B. escorts service personnel at all times when performing their work.
C. performs maintenance during noncritical processing times.
D. independently verifies that maintenance is being performed.

C is the correct answer.

Justification:

A. While the trustworthiness of the service personnel is important, it is normal practice for these individuals to be escorted and supervised by the data center personnel. It is also expected that the service provider would perform this background check, not the customer.
B. Escorting service personnel is common and a good practice, but the greater risk in this case would be if work were performed during critical processing times.
C. The biggest risk to normal operations in a data center would be if an incident or mishap were to happen during critical peak processing times; therefore, it would be prudent to ensure that no type of system maintenance be performed at these critical times.
D. It is possible that the service provider is performing inadequate maintenance; therefore, this issue may need to be investigated; however, the bigger risk is maintenance being performed at critical processing times.

A4-141 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?

A. Virtual tape libraries
B. Disk-based snapshots
C. Continuous data backup
D. Disk-to-tape backup

C is the correct answer.

Justification:

A. Virtual tape libraries would require time to complete the backup, while continuous data backup happens online (in real time).
B. Disk-based snapshots would require time to complete the backup and would lose some data between the times of the backup and the failure, while continuous data backup happens online (in real time).
C. Recovery point objective (RPO) is based on the acceptable data loss in the case of a disruption. In this scenario the organization needs a short RPO and continuous data backup is the best option.
D. Disk-to-tape backup would require time to complete the backup, while continuous data backup happens online (in real time).

A4-142 A lower recovery time objective results in:

A. higher disaster tolerance.
B. higher cost.
C. wider interruption windows.
D. more permissive data loss.

B is the correct answer.

Justification:

A. Disaster tolerance relates the length of time that critical business processes can be interrupted. A higher disaster tolerance allows for a longer outage and, therefore, longer recovery time.
B. Recovery time objective (RTO) is based on the acceptable down time in case of a disruption of operations. The lower the RTO, the higher the cost of recovery strategies.
C. The lower the disaster tolerance, the narrower the interruption windows. The interruption window is the length of the outage of critical processes.
D. Permissive data loss relates to recovery point objective, not disaster tolerance.

A4-143 During an implementation review of a recent application deployment, it was determined that several incidents were assigned incorrect priorities and, because of this, failed to meet the business service level agreement (SLA). What is the **GREATEST** concern?

A. The support model was not approved by senior management.
B. The incident resolution time specified in the SLA is not realistic.
C. There are inadequate resources to support the applications.
D. The support model was not properly developed and implemented.

D is the correct answer.

Justification:

A. While senior management involvement is important, the more critical issue is whether the support model was not properly developed and implemented.
B. While the incident resolution time specified in the service level agreement may not always be attainable, the more critical issue is whether the support model was not properly developed and implemented.
C. While adequate support resources are important, the more critical issue is whether the support model was not properly developed and implemented.
D. The greatest concern for the IS auditor is that the support model was not developed and implemented correctly to prevent or react to potential outages. Incidents could cost the business a significant amount of money and a support model should be implemented with the project. This should be a step within the system development life cycle and procedures and, if it is missed on one project, it may be a symptom of an overall breakdown in process.

A4-144 What is the **BEST** backup strategy for a large database with data supporting online sales?

A. Weekly full backup with daily incremental backup
B. Daily full backup
C. Clustered servers
D. Mirrored hard disks

D is the correct answer.

Justification:

A. Weekly full backup and daily incremental backup is a poor backup strategy for online transactions. Because this system supports online sales it can be difficult to recreate lost data and this solution may result in a loss of up to one day's worth of data.
B. A full backup normally requires a couple of hours, and therefore, it can be impractical to conduct a full backup every day.
C. Clustered servers provide a redundant processing capability but are not a backup.
D. Mirrored hard disks will ensure that all data are backed up to more than one disk so that a failure of one disk will not result in loss of data.

A4-145 An IS auditor notes during an audit that an organization's business continuity plan (BCP) does not adequately address information confidentiality during the recovery process. The IS auditor should recommend that the plan be modified to include:

A. the level of information security required when business recovery procedures are invoked.
B. information security roles and responsibilities in the crisis management structure.
C. information security resource requirements.
D. change management procedures for information security that could affect business continuity arrangements.

A is the correct answer.

Justification:

A. **Business should consider whether information security levels required during recovery should be the same, lower or higher than when business is operating normally. In particular, any special rules for access to confidential data during a crisis need to be identified.**
B. During a time of crisis, the security needs of the organization may increase because many usual controls such as separation of duties are missing. Having security roles in the crisis management plan is important, but that is not the best answer to this scenario.
C. Identifying the resource requirements for information security, as part of the business continuity plan (BCP), is important, but it is more important to set out the security levels that would be required for protected information.
D. Change management procedures can help keep a BCP up to date but are not relevant to this scenario.

A4-146 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:

A. event error log generated at the disaster recovery site.
B. disaster recovery test plan.
C. disaster recovery plan.
D. configurations and alignment of the primary and disaster recovery sites.

D is the correct answer.

Justification:

A. If the issue cannot be clarified, the IS auditor should then review the event error log.
B. The disaster recovery test plan would not identify any issues related to system performance unless the test was poorly designed and inefficient, but that would come after checking the configuration.
C. Reviewing the disaster recovery plan would be unlikely to provide any information about system performance issues.
D. **Because the configuration of the system is the most probable cause, the IS auditor should review that first.**

A4-147 Which of the following is the **GREATEST** risk when storage growth in a critical file server is not managed properly?

A. Backup time would steadily increase.
B. Backup operational costs would significantly increase.
C. Storage operational costs would significantly increase.
D. Server recovery work may not meet the recovery time objective.

D is the correct answer.

Justification:
A. Backup time may increase, but that can be managed. The most important issue is the time taken to recover the data.
B. The backup cost issues are not as significant as not meeting the recovery time objective (RTO).
C. The storage cost issues are not as significant as not meeting the RTO.
D. In case of a crash, recovering a server with an extensive amount of data could require a significant amount of time. If the recovery cannot meet the RTO, there will be a discrepancy in IT strategies. It is important to ensure that server restoration can meet the RTO.

A4-148 An organization has a business process with a recovery time objective equal to zero and a recovery point objective close to one minute. This implies that the process can tolerate:

A. a data loss of up to one minute, but the processing must be continuous.
B. a one-minute processing interruption but cannot tolerate any data loss.
C. a processing interruption of one minute or more.
D. both a data loss and a processing interruption longer than one minute.

A is the correct answer.

Justification:
A. Recovery time objective (RTO) measures an organization's tolerance for downtime and recovery point objective (RPO) measures how much data loss can be accepted.
B. A processing interruption of one minute would exceed the zero RTO set by the organization.
C. A processing interruption of one minute or more would exceed the continuous availability requirements of an RTO of zero.
D. An RPO of one minute would only allow data loss of one minute.

A4-149 Which of the following issues should be the **GREATEST** concern to the IS auditor when reviewing an IT disaster recovery test?

A. 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.
B. During the test, some of the backup systems were defective or not working, causing the test of these systems to fail.
C. The procedures to shut down and secure the original production site before starting the backup site required far more time than planned.
D. Every year, the same employees perform the test. The recovery plan documents are not used because every step is well known by all participants.

B is the correct answer.

Justification:
A. This is not a concern because over the course of the year, all the systems were tested.
B. The purpose of the test is to test the backup plan. When the backup systems are not working then the plan cannot be counted on in a real disaster. This is the most serious problem.
C. In a real disaster, there is no need for a clean shutdown of the original production environment because the first priority is to bring the backup site up.
D. 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 because a disaster can occur when they are not available. However, the fact that the test works is less serious than the failure of the systems and infrastructure that the recovery plan counts on. Good practice would rotate different people through the test and ensure that the plan itself is followed and tested.

A4-150 The frequent updating of which of the following is key to the continued effectiveness of a disaster recovery plan?

A. Contact information of key personnel
B. Server inventory documentation
C. Individual roles and responsibilities
D. Procedures for declaring a disaster

A is the correct answer.

Justification:
A. 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.
B. Asset inventory is important and should be linked to the change management process of the organization but having access to key people may compensate for outdated records.
C. Individual roles and responsibilities are important, but in a disaster many people could fill different roles depending on their experience.
D. The procedures for declaring a disaster are important because this can affect response, customer perception and regulatory issues, but not as important as having the right people there when needed.

A4-151 A live test of a mutual agreement for IT system recovery has been carried out, including a four-hour test of intensive usage by the business units. The test has been successful, but gives only partial assurance that the:

A. system and the IT operations team can sustain operations in the emergency environment.
B. resources and the environment could sustain the transaction load.
C. connectivity to the applications at the remote site meets response time requirements.
D. workflow of actual business operations can use the emergency system in case of a disaster.

A is the correct answer.

Justification:
A. The applications have been operated intensively, but the capability of the system and the IT operations team to sustain and support this environment (ancillary operations, batch closing, error corrections, output distribution, etc.) is only partially tested.
B. Because the test involved intensive usage, the backup would seem to be able to handle the transaction load.
C. Because users were able to connect to and use the system, the response time must have been satisfactory.
D. The intensive tests by the business indicated that the workflow systems worked correctly. Changes to the environment could pose a problem in the future, but it is working correctly now.

A4-152 Which of the following is the **MOST** important consideration when defining recovery point objectives?

A. Minimum operating requirements
B. Acceptable data loss
C. Mean time between failures
D. Acceptable time for recovery

B is the correct answer.

Justification:
A. Minimum operating requirements help define recovery strategies.
B. Recovery point objectives are the level of data loss/reworking an organization is willing to accept.
C. Mean time between failures helps define likelihood of system failure.
D. Recovery time objectives are the acceptable time delay in availability of business operations.

A4-153 To address an organization's disaster recovery requirements, backup intervals should not exceed the:

A. service level objective.
B. recovery time objective.
C. recovery point objective.
D. maximum acceptable outage.

C is the correct answer.

Justification:
A. Organizations will try to set service level objective to meet established business targets. The resulting time for the service level agreement relates to recovery of services, not to recovery of data.
B. Recovery time objective (RTO) defines the time period after the disaster in which normal business functionality needs to be restored.
C. Recovery point objective defines the point in time to which data must be restored after a disaster to resume processing transactions. Backups should be performed in a way that the latest backup is no older than this maximum time frame. If the backups are not done frequently enough, then too many data are likely to be lost.
D. Maximum acceptable outage (MAO) is the maximum amount of system downtime that is tolerable. It can be used as a synonym for maximum tolerable period of disruption or maximum allowable downtime. However, the RTO denotes an objective/target, while the MAO constitutes a vital necessity for an organization's survival.

A4-154 The **FIRST** step in the execution of a problem management mechanism should be:

A. issue analysis.
B. exception ranking.
C. exception reporting.
D. root cause analysis.

C is the correct answer.

Justification:
A. Analysis and resolution are performed after logging and triage have been performed.
B. Exception ranking can only be performed once the exceptions have been reported.
C. The reporting of operational issues is normally the first step in tracking problems.
D. Root cause analysis is performed once the exceptions have been identified and is not normally the first part of problem management.

A4-155 Which of the following would **BEST** support 24/7 availability?

A. Daily backup
B. Offsite storage
C. Mirroring
D. Periodic testing

C is the correct answer.

Justification:
A. Daily backup implies that it is reasonable for restoration to take place within a number of hours but not immediately.
B. Offsite storage does not, itself, support continuous availability.
C. Mirroring of critical elements is a tool that facilitates immediate (failover) recoverability.
D. Periodic testing of systems does not, itself, support continuous availability.

A4-156 The **PRIMARY** purpose of implementing Redundant Array of Inexpensive Disks (RAID) level 1 in a file server is to:

A. achieve performance improvement.
B. provide user authentication.
C. ensure availability of data.
D. ensure the confidentiality of data.

C is the correct answer.

Justification:
A. Redundant Array of Inexpensive Disks (RAID) level 1 does not improve performance. It writes the data to two separate disk drives.
B. RAID level 1 has no relevance to authentication.
C. **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.**
D. RAID level 1 does nothing to provide for data confidentiality.

A4-157 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:

A. physically separated from the data center and not subject to the same risk.
B. given the same level of protection as that of the computer data center.
C. outsourced to a reliable third party.
D. equipped with surveillance capabilities.

A is the correct answer.

Justification:
A. **It is important that there is an offsite storage location for IS files and that it is in a location not subject to the same risk as the primary data center.**
B. The offsite location may be shared with other companies and, therefore, have an even higher level of protection than the primary data center.
C. An offsite location may be owned by a third party or by the organization itself.
D. Physical protection is important but not as important as not being affected by the same crisis.

A4-158 If a database is restored using before-image dumps, where should the process begin following an interruption?

A. Before the last transaction
B. After the last transaction
C. As the first transaction after the latest checkpoint
D. As the last transaction before the latest checkpoint

A is the correct answer.

Justification:
A. **If before images are used, the last transaction in the dump will not have updated the database prior to the dump being taken.**
B. The last transaction will not have updated the database and must be reprocessed.
C. Program checkpoints are irrelevant in this situation. Checkpoints are used in application failures.
D. Program checkpoints are irrelevant in this situation. Checkpoints are used in application failures.

A4-159 In addition to the backup considerations for all systems, which of the following is an important consideration in providing backup for online systems?

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

B is the correct answer.

Justification:

A. Maintaining system software parameters is important for all systems, not just online systems.
B. Ensuring periodic dumps of transaction logs is the only safe way of preserving timely historic data. Because online systems do not have a paper trail that can be used to recreate data, maintaining transaction logs is critically important to prevent data loss. The volume of activity usually associated with an online system may make other more traditional methods of backup impractical.
C. Having generations of backups is a good practice for all systems.
D. All backups should consider offsite storage at a location that is accessible but not likely to be affected by the same disaster.

A4-160 Which of the following disaster recovery testing techniques is the **MOST** efficient way to determine the effectiveness of the plan?

A. Preparedness tests
B. Paper tests
C. Full operational tests
D. Actual service disruption

A is the correct answer.

Justification:

A. Preparedness tests involve simulation of the entire environment (in phases) at relatively low cost and help the team to better understand and prepare for the actual test scenario.
B. Paper tests in a walk-through test the entire plan, but there is no simulation and less is learned. It also is difficult to obtain evidence that the team has understood the test plan.
C. Full operational tests would require approval from management, are not easy or practical to test in most scenarios and may trigger a real disaster.
D. An actual service disruption is not recommended in most cases unless required by regulation or policy.

A4-161 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:

A. database integrity checks.
B. validation checks.
C. input controls.
D. database commits and rollbacks.

D is the correct answer.

Justification:
A. Database integrity checks are important to ensure database consistency and accuracy. These include isolation, concurrency and durability controls, but the most important issue here is atomicity—the requirement for transactions to complete entirely and commit or else roll back to the last known good point.
B. Validation checks will prevent introduction of corrupt data but will not address system failure.
C. Input controls are important to protect the integrity of input data but will not address system failure.
D. Database commits ensure that the data are saved after the transaction processing is completed. Rollback ensures that the processing that has been partially completed as part of the transaction is reversed back and not saved if the entire transaction does not complete successfully.

A4-162 Which of the following security measures **BEST** ensures the integrity of information stored in a data warehouse?

A. Validated daily backups
B. Change management procedures
C. Data dictionary maintenance
D. A read-only restriction

D is the correct answer.

Justification:
A. Backups address availability, not integrity. Validated backups ensure that the backup will work when needed.
B. Adequate change management procedures protect the data warehouse and the systems with which the data warehouse interfaces from unauthorized changes but are not usually concerned with the data.
C. Data dictionary maintenance procedures provide for the definition and structure of data that are input to the data warehouse. This will not affect the integrity of data already stored.
D. Because most data in a data warehouse are historic and do not need to be changed, applying read-only restrictions prevents data manipulation.

A4-163 Which of the following ensures the availability of transactions in the event of a disaster?

A. Send hourly tapes containing transactions offsite.
B. Send daily tapes containing transactions offsite.
C. Capture transactions to multiple storage devices.
D. Transmit transactions offsite in real time.

D is the correct answer.

Justification:
A. Sending hourly tapes containing transactions offsite is not in real time and, therefore, would possibly result in the loss of one hour's worth of transactional data.
B. Sending daily tapes containing transactions offsite is not in real time and, therefore, could result in the loss of one day's worth of transactional data.
C. Capturing transactions to multiple storage devices does not ensure availability at an offsite location.
D. The only way to ensure availability of all transactions is to perform a real-time transmission to an offsite facility.

A4-164 IT 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:

A. upgrading to a level 5 RAID.
B. increasing the frequency of onsite backups.
C. reinstating the offsite backups.
D. establishing a cold site in a secure location.

C is the correct answer.

Justification:

A. Upgrading to level 5 Redundant Array of Inexpensive Disks (RAID) will not address the problem of catastrophic failure of the data center housing all the data.
B. Increasing the frequency of onsite backups is not relevant to RAID 1 because all data are being mirrored already.
C. A RAID system, at any level, will not protect against a natural disaster. The problem will not be alleviated without offsite backups.
D. A cold site is an offsite recovery location but will not provide for data recovery because a cold site is not used to store data.

A4-165 In a contract with a hot, warm or cold site, contractual provisions should **PRIMARILY** cover which of the following considerations?

A. Physical security measures
B. Total number of subscribers
C. Number of subscribers permitted to use a site at one time
D. References by other users

C is the correct answer.

Justification:

A. Physical security measures are not always part of the contract, although they are an important consideration when choosing a third-party site.
B. The total number of subscribers is a consideration, but more important is whether the agreement limits the number of subscribers in a building or in a specific area. It is also good to know if other subscribers are competitors.
C. The contract should specify the number of subscribers permitted to use the site at any one time. The contract can be written to give preference to certain subscribers.
D. The references that other users can provide are a consideration taken before signing the contract; it is by no means part of the contractual provisions.

A4-166 Which of the following reports is the **MOST** appropriate source of information for an IS auditor to validate that an Internet service provider (ISP) has been complying with an enterprise service level agreement for the availability of outsourced telecommunication services?

A. Downtime reports on the telecommunication services generated by the ISP
B. A utilization report of automatic failover services generated by the enterprise
C. A bandwidth utilization report provided by the ISP
D. Downtime reports on the telecommunication services generated by the enterprise

D is the correct answer.

Justification:

A. The Internet service provider (ISP)-generated downtime reports are produced by the same entity that is being monitored. As a result, it will be necessary to review these reports for possible bias and/or errors against other data.
B. The information provided by these reports is indirect evidence of the extent that the backup telecommunication services were used. These reports may not indicate compliance with the service level agreement, just that the failover systems had been used.
C. Utilization reports are used to measure the usage of bandwidth, not uptime.
D. The enterprise should use internally generated downtime reports to monitor the service provided by the ISP and, as available, to compare with the reports provided by the ISP.

A4-167 Integrating the business continuity plan into IT project management aids in:

A. the testing of the business continuity requirements.
B. the development of a more comprehensive set of requirements.
C. the development of a transaction flowchart.
D. ensuring the application meets the user's needs.

B is the correct answer.

Justification:

A. Testing the business continuity plan's (BCP) requirements is not related to IT project management.
B. Integrating the BCP into the development process ensures complete coverage of the requirements through each phase of the project.
C. A transaction flowchart aids in analyzing an application's controls but does not affect business continuity.
D. A BCP will not directly address the detailed processing needs of the users.

A4-168 An enterprise uses privileged accounts to process configuration changes for mission-critical applications. Which of the following would be the **BEST** and appropriate control to limit the risk in such a situation?

A. Ensure that audit trails are accurate and specific.
B. Ensure that personnel have adequate training.
C. Ensure that personnel background checks are performed for critical personnel.
D. Ensure that supervisory approval and review are performed for critical changes.

D is the correct answer.

Justification:
A. Audit trails are a detective control and, in many cases, can be altered by those with privileged access.
B. Staff proficiency is important and good training may be somewhat of a deterrent, but supervisory approval and review is the best choice.
C. Performing background checks is a very basic control and will not effectively prevent or detect errors or malfeasance.
D. Supervisory approval and review of critical changes by the accountable managers in the enterprise are required to avoid and detect any unauthorized change. In addition to authorization, supervision enforces a separation of duties and prevents an unauthorized attempt by any single employee.

A4-169 An IS auditor observed that multiple applications are hosted on the same server. The recovery time objective (RTO) for the server will be:

A. based on the application with the longest RTO.
B. based on the application with the shortest RTO.
C. based on the mean of each application's RTO.
D. independent of the RTO and based on the criticality of the application.

B is the correct answer.

Justification:
A. The longest recovery time objective (RTO) will be determined for noncritical applications, which will not help in meeting the objectives for critical systems.
B. When several applications are hosted on a server, the server's RTO must be determined by taking the RTO of the most critical application, which is the shortest RTO.
C. The mean value will be higher than the RTO for a critical application.
D. Critical applications usually have the shortest RTOs. The RTO of the server cannot be independent of the application RTO.

A4-170 During an application audit, the IS auditor finds several problems related to corrupt data in the database. Which of the following is a corrective control that the IS auditor should recommend?

A. Define the standards, and closely monitor them for compliance.
B. Ensure that only authorized personnel can update the database.
C. Establish controls to handle concurrent access problems.
D. Proceed with restore procedures.

D is the correct answer.

Justification:
A. Establishing standards is a preventive control, and monitoring for compliance is a detective control.
B. Ensuring that only authorized personnel can update the database is a preventive control.
C. Establishing controls to handle concurrent access problems is a preventive control.
D. Proceeding with restore procedures is a corrective control. Restore procedures can be used to recover databases to their last-known archived version.

A4-171 Which of the following scenarios provides the **BEST** disaster recovery plan to implement for critical applications?

A. Daily data backups that are stored offsite and a hot site located 140 kilometers from the main data center
B. Daily data backups that are stored onsite in a fireproof safe
C. Real-time data replication between the main data center and the hot site located 500 meters from the main site
D. Daily data backups that are stored offsite with a warm site located 70 kilometers from the main data center

A is the correct answer.

Justification:
A. Of the given choices, this is the most suitable answer. The disaster recovery plan includes a hot site that is located sufficiently away from the main data center and will allow recovery in the event of a major disaster. Not having real-time backups may be a problem depending on recovery point objective (RPO).
B. Having data backups is necessary, but not having a replication site would be insufficient for the critical application.
C. Depending on the type of disaster, a hot site should normally be located more than 500 meters from the main facility. Having real-time backups may be the best option though, depending on the data RPO.
D. A warm site may take days to recover, and therefore, it may not be a suitable solution.

A4-172 Which of the following is the **BEST** indicator of the effectiveness of backup and restore procedures while restoring data after a disaster?

A. Members of the recovery team were available.
B. Recovery time objectives were met.
C. Inventory of backup tapes was properly maintained.
D. Backup tapes were completely restored at an alternate site.

B is the correct answer.

Justification:
A. The availability of key personnel does not ensure that backup and restore procedures will work effectively.
B. The effectiveness of backup and restore procedures is best ensured by recovery time objectives (RTOs) being met because these are the requirements that are critically defined during the business impact analysis stage, with the inputs and involvement of all business process owners.
C. The inventory of the backup tapes is only one element of the successful recovery.
D. The restoration of backup tapes is a critical success, but only if they were able to be restored within the time frames set by the RTO.

A4-173 Which of the following would be the **MOST** appropriate recovery strategy for a sensitive system with a high recovery time objective (RTO)?

A. Warm site
B. Hot site
C. Cold site
D. Mobile recovery site

C is the correct answer.

Justification:
A. While a warm site may be a good solution, it would not be the most appropriate because it is more expensive than a cold site.
B. A hot site is used for those systems classified as critical that have a low recovery time objective (RTO).
C. Sensitive systems having a high RTO can be performed manually at a tolerable cost for an extended period of time. The cold site would be the most cost-effective solution for such a system.
D. A mobile recovery site would not be as cost-effective as a cold site and would not be appropriate for systems with high RTOs.

A4-174 Which of the following should an incident response team address **FIRST** after a major incident in an information processing facility?

A. Restoration at the facility
B. Documentation of the facility
C. Containment at the facility
D. Monitoring of the facility

C is the correct answer.

Justification:
A. Restoration ensures that the affected systems or services are restored to a condition specified in the restore point objective. This action will be possible only after containment of the damage.
B. Documentation of the facility should be prepared to inform management of the incident; however, damage must be contained first.
C. The first priority (after addressing life safety) is the containment of the incident at the facility so that spread of the damage is minimized. The incident team must gain control of the situation.
D. Monitoring of the facility is important, although containment must take priority to avoid spread of the damage.

A4-175 An IS auditor discovers that some hard drives disposed of by an enterprise were not sanitized in a manner that would reasonably ensure the data could not be recovered. In addition, the enterprise does not have a written policy on data disposal. The IS auditor should **FIRST**:

A. draft an audit finding and discuss it with the auditor in charge.
B. determine the sensitivity of the information on the hard drives.
C. discuss with the IT manager good practices in data disposal.
D. develop an appropriate data disposal policy for the enterprise.

B is the correct answer.

Justification:
A. Drafting a finding without a quantified risk would be premature.
B. Even though a policy is not available, the IS auditor should determine the nature of the information on the hard drives to quantify, as much as possible, the risk.
C. It would be premature to discuss good practices with the IT manager until the extent of the incident has been quantified.
D. An IS auditor should not develop policies.

A4-176 An IS auditor is assessing services provided by an Internet service provider (ISP) during an IS compliance audit of a nationwide corporation that operates a governmental program. Which of the following is **MOST** important?

A. Review the request for proposal.
B. Review monthly performance reports generated by the ISP.
C. Review the service level agreement.
D. Research other clients of the ISP.

C is the correct answer.

Justification:
A. Because the request for proposal is not the contracted agreement, it is more relevant to review the terms of the SLA.
B. The reports from the Internet service provider (ISP) are indirect evidence that may require further review to ensure accuracy and completeness.
C. **A service level agreement provides the basis for an adequate assessment of the degree to which the provider is meeting the level of agreed-on service.**
D. The services provided to other clients of the ISP are irrelevant to the IS auditor.

A4-177 During an audit of a small enterprise, the IS auditor noted that the IS director has superuser-privilege access that allows the director to process requests for changes to the application access roles (access types). Which of the following should the IS auditor recommend?

A. Implement a properly documented process for application role change requests.
B. Hire additional staff to provide a segregation of duties for application role changes.
C. Implement an automated process for changing application roles.
D. Document the current procedure in detail and make it available on the enterprise intranet.

A is the correct answer.

Justification:
A. **The IS auditor should recommend implementation of processes that could prevent or detect improper changes from being made to the major application roles. The application role change request process should start and be approved by the business owner; then, the IS director can make the changes to the application.**
B. While it is preferred that a strict segregation of duties be adhered to and that additional staff be recruited, this practice is not always possible in small enterprises. The IS auditor must look at recommended alternative processes.
C. An automated process for managing application roles may not be practical to prevent improper changes being made by the IS director, who also has the most privileged access to the application.
D. Making the existing process available on the enterprise intranet would not provide any value to protect the system.

A4-178 While observing a full simulation of the business continuity plan, an IS auditor notices that the notification systems within the organizational facilities could be severely impacted by infrastructure damage. The **BEST** recommendation the IS auditor can provide to the organization is to ensure:

A. the salvage team is trained to use the notification system.
B. the notification system provides for the recovery of the backup.
C. redundancies are built into the notification system.
D. the notification systems are stored in a vault.

C is the correct answer.

Justification:
A. The salvage team would not be able to use a severely damaged notification system, even if they are trained to use it.
B. The recovery of the backups has no bearing on the notification system.
C. **If the notification system has been severely impacted by the damage, redundancy would be the best control.**
D. Storing the notification system in a vault would be of little value if the building is damaged.

A4-179 To ensure structured disaster recovery, it is **MOST** important that the business continuity plan and disaster recovery plan are:

A. stored at an alternate location.
B. communicated to all users.
C. tested regularly.
D. updated regularly.

C is the correct answer.

Justification:
A. Storing the business continuity plan (BCP) at an alternate location is useful in the case of complete site outage; however, the BCP is not useful during a disaster without adequate tests.
B. Communicating to users is not of much use without actual tests.
C. **If the BCP is tested regularly, the BCP and disaster recovery plan team is adequately aware of the process and that helps in structured disaster recovery.**
D. Even if the plan is updated regularly, it is of less use during an actual disaster if it is not adequately tested.

A4-180 The **PRIMARY** purpose of a business impact analysis is to:

A. define recovery strategies.
B. identify the alternate site.
C. improve recovery testing.
D. calculate the annual loss expectancy.

A is the correct answer.

Justification:
A. **One of the primary outcomes of a business impact analysis (BIA) is the recovery time objective and the recovery point objective, which help in defining the recovery strategies.**
B. A BIA, itself, will not help in identifying the alternate site. That is determined during the recovery strategy phase of the project.
C. A BIA, itself, will not help improve recovery testing. That is done during the implementation and testing phase of the project.
D. The annual loss expectancy of critical business assets and processes is determined during risk assessment and will be reviewed in the BIA, but this is not the primary advantage.

A4-181 Which of the following **BEST** helps define disaster recovery strategies?

A. Annual loss expectancy and exposure factor
B. Maximum tolerable downtime and data loss
C. Existing server and network redundancies
D. Data backup and offsite storage requirements

B is the correct answer.

Justification:
A. Annual loss expectancy and exposure factor are more related to risk in general.
B. One of the key outcomes of the business impact analysis is the recovery time objective (RTO) and recovery point objective (RPO)—maximum tolerable downtime and data loss—that further help in identifying the recovery strategies.
C. Existing server and network redundancies are good to know, but the RTO and RPO are needed to design the right recovery strategies.
D. Data backup and offsite storage requirements are an important aspect of a business continuity plan, but these alone will not help in defining the disaster recovery strategies.

A4-182 After a disaster declaration, the media creation date at a warm recovery site is based on the:

A. recovery point objective.
B. recovery time objective.
C. service delivery objective.
D. maximum tolerable outage.

A is the correct answer.

Justification:
A. The recovery point objective (RPO) is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption. The media creation date will reflect the point to which data are to be restored or the RPO.
B. The recovery time objective is the amount of time allowed for the recovery of a business function or resource after a disaster occurs.
C. The service delivery objective is directly related to the business needs and is the level of service to be reached during the alternate process mode until the normal situation is restored.
D. The maximum tolerable outage is the maximum time that an organization can support processing in alternate mode.

A4-183 The activation of an enterprise's business continuity plan should be based on predetermined criteria that address the:

A. duration of the outage.
B. type of outage.
C. probability of the outage.
D. cause of the outage.

A is the correct answer.

Justification:

A. **The initiation of a business continuity plan (action) should primarily be based on the maximum period for which a business function can be disrupted before the disruption threatens the achievement of organizational objectives.**
B. The type of outage is not as important to the activation of the plan as the length or duration of the outage.
C. The probability of the outage would be relevant to the frequency of incidents, not the need to activate the plan. The plan is designed to be activated after an event of a certain duration occurs.
D. The cause of the outage may affect the response plan to be activated, but not the decision to activate the plan. The plan will be activated any time an event of a predetermined duration occurs.

A4-184 During an audit of a small company that provides medical transcription services, an IS auditor observes several issues related to the backup and restore process. Which of the following should be the auditor's **GREATEST** concern?

A. Restoration testing for backup media is not performed; however, all data restore requests have been successful.
B. The policy for data backup and retention has not been reviewed by the business owner for the past three years.
C. The company stores transcription backup tapes offsite using a third-party service provider, which inventories backup tapes annually.
D. Failed backup alerts for the marketing department data files are not followed up on or resolved by the IT administrator.

C is the correct answer.

Justification:

A. Lack of restoration testing does not increase the risk of unauthorized leakage of information. Not performing restoration tests on backup tapes poses a risk; however, this risk is somewhat mitigated because past data restore requests have been successful.
B. Lack of review of the data backup and retention policy may be of a concern if systems and business processes have changed in the past three years. The IS auditor should perform additional procedures to verify the validity of existing procedures. In addition, lack of this control does not introduce a risk of unauthorized leakage of information.
C. **For a company working with confidential patient data, the loss of a backup tape is a significant incident. Privacy laws specify severe penalties for such an event, and the company's reputation could be damaged due to mandated reporting requirements. To gain assurance that tapes are being handled properly, the organization should perform audit tests that include frequent physical inventories and an evaluation of the controls in place at the third-party provider.**
D. Failed backup alerts that are not followed up on and resolved imply that certain data or files are not backed up. This is a concern if the files/data being backed up are critical in nature, but, typically, marketing data files are not regulated in the same way as medical transcription files. Lack of this control does not introduce a risk of unauthorized leakage of sensitive information.

A4-185 Determining the service delivery objective should be based **PRIMARILY** on:

A. the minimum acceptable operational capability.
B. the cost-effectiveness of the restoration process.
C. meeting the recovery time objectives.
D. the allowable interruption window.

A is the correct answer.

Justification:

A. **The service delivery objective (SDO) is the level of service to be reached during the alternate process mode until the normal situation is restored. This is directly related to the business needs.**
B. The cost-effectiveness of the restoration process is not the main consideration of determining the SDO.
C. Meeting the recovery time objective may be one of the considerations in determining the SDO, but it is a secondary factor.
D. The allowable interruption window may be one of the factors secondary to determining the SDO.

A4-186 An IS auditor reviewing the application change management process for a large multinational company should be **MOST** concerned when:

A. test systems run different configurations than do production systems.
B. change management records are paper based.
C. the configuration management database is not maintained.
D. the test environment is installed on the production server.

C is the correct answer.

Justification:

A. While, ideally, production and test systems should be configured identically, there may be reasons why this does not occur. The more significant concern is whether the configuration management database was not maintained.
B. Paper-based change management records are inefficient to maintain and not easy to review in large volumes; however, they do not present a concern from a control point of view as long as they are properly and diligently maintained.
C. **The configuration management database (CMDB) is used to track configuration items (CIs) and the dependencies between them. An out-of-date CMDB in a large multinational company could result in incorrect approvals being obtained or leave out critical dependencies during the test phase.**
D. While it is not ideal to have the test environment installed on the production server, it is not a control-related concern. As long as the test and production environments are kept separate, they can be installed on the same physical server(s).

A4-187 An IS auditor can verify that an organization's business continuity plan (BCP) is effective by reviewing the:

A. alignment of the BCP with industry good practices.
B. results of business continuity tests performed by IS and end-user personnel.
C. offsite facility, its contents, security and environmental controls.
D. annual financial cost of the BCP activities versus the expected benefit of the implementation of the plan.

B is the correct answer.

Justification:
A. Alignment of the business continuity plan (BCP) with industry good practices does not provide the assurance of the effectiveness of the BCP.
B. The effectiveness of the BCP can best be evaluated by reviewing the results from previous business continuity tests for thoroughness and accuracy in accomplishing their stated objectives.
C. The offsite facility, its contents, security and environmental controls do not provide the assurance of the effectiveness of the BCP. Only testing will provide an accurate assessment of the effectiveness of the BCP.
D. The annual financial cost of the BCP activities versus the expected benefit of implementation of the plan does not provide the assurance of the effectiveness of the BCP. Only testing will provide an accurate assessment of the effectiveness of the BCP.

A4-188 It is **MOST** appropriate to implement an incremental backup scheme when:

A. there is limited recovery time for critical data.
B. online disk-based media are preferred.
C. there is limited media capacity.
D. a random selection of backup sets is required.

C is the correct answer.

Justification:
A. A full backup or differential backup is preferred in this situation.
B. Incremental backup could be used irrespective of the media adopted.
C. In an incremental backup, after the full backup, only the files that have changed are backed up, thus minimizing media storage.
D. A random selection of backup sets may not be possible with an incremental backup scheme because only fragments of the data are backed up on a daily basis.

A4-189 Which of the following **BEST** mitigates the risk arising from using reciprocal agreements as a recovery alternative?

A. Perform disaster recovery exercises annually.
B. Ensure that partnering organizations are separated geographically.
C. Regularly perform a business impact analysis.
D. Select a partnering organization with similar systems.

B is the correct answer.

Justification:
A. While disaster recovery exercises are important but difficult to perform in a reciprocal agreement, the greater risk is geographic proximity.
B. If the two partnering organizations are in close geographic proximity, this could lead to both organizations being subjected to the same environmental disaster, such as an earthquake.
C. A business impact analysis will help both organizations identify critical applications, but separation is a more important consideration when entering reciprocal agreements.
D. Selecting a partnering organization with similar systems is a good idea, but separation is a more important consideration when entering reciprocal agreements.

A4-190 During the review of an in-house developed application, the **GREATEST** concern to an IS auditor is if a:

A. user raises a change request and tests it in the test environment.
B. programmer codes a change in the development environment and tests it in the test environment.
C. manager approves a change request and then reviews it in production.
D. manager initiates a change request and subsequently approves it.

D is the correct answer.

Justification:
A. Having a user involved in testing changes is common practice.
B. Having a programmer code a change in development and then separately test the change in a test environment is a good practice and preferable over testing in production.
C. Having a manager review a change to make sure it was done correctly is an acceptable practice.
D. Initiating and subsequently approving a change request violates the principle of segregation of duties. A person should not be able to approve their own requests.

A4-191 In a disaster recovery situation, which of the following is the **MOST** important metric to ensure that data are synchronized between critical systems?

A. Recovery point objective
B. Recovery time objective
C. Recovery service resilience
D. Recovery service scalability

A is the correct answer.

Justification:
A. Establishing a common recovery point objective is most critical for ensuring that interdependencies between systems are properly synchronized. It ensures that systems do not contain data from different points in time that may result in accounting transactions that cannot be reconciled and a loss of referential integrity.
B. Recovery time objectives are not as important to synchronize because they normally vary depending on the level of effort and resources required to restore a system.
C. Recovery service resilience measures the fault tolerance due to data exceptions and ability to restart and recover from internal failures.
D. Recovery service scalability refers to the capacity constraints and limitations that a recovery solution may have relative to the original system configuration.

A4-192 Which of the following **BEST** mitigates the risk of backup media containing irreplaceable information being lost or stolen while in transit?

A. Ensure that media are encrypted.
B. Maintain a duplicate copy.
C. Maintain chain of custody.
D. Ensure that personnel are bonded.

B is the correct answer.

Justification:
A. Although strong encryption protects against disclosure, it will not mitigate the loss of irreplaceable data.
B. Sensitive data should always be fully backed up before being transmitted or moved. Backups of sensitive information should be treated with the same control considerations as the actual data.
C. Chain of custody is an important control, but it will not mitigate a loss if a locked area is broken into and media removed or if media are lost while in an individual's custody.
D. Bonded security, although good for preventing theft, will not protect against accidental loss or destruction.

A4-193 An IS auditor is reviewing the change management process for an enterprise resource planning application. Which of the following is the **BEST** method for testing program changes?

A. Select a sample of change tickets and review them for authorization.
B. Perform a walk-through by tracing a program change from start to finish.
C. Trace a sample of modified programs to supporting change tickets.
D. Use query software to analyze all change tickets for missing fields.

C is the correct answer.

Justification:

A. Selecting a sample of change tickets and reviewing them for authorization helps test for authorization controls; however, it does not identify program changes that were made without supporting change tickets.
B. Performing a walk-through assists the IS auditor in understanding the process but does not ensure that all changes adhere to the normal process.
C. **Tracing a sample of modified programs to supporting change tickets is the best way to test change management controls. This method is most likely to identify instances in which a change was made without supporting documentation.**
D. Using query software to analyze all change tickets for missing fields does not identify program changes that were made without supporting change tickets.

A4-194 Emergency changes that bypass the normal change control process are **MOST** acceptable if:

A. management reviews and approves the changes after they have occurred.
B. the changes are reviewed by a peer at the time of the change.
C. the changes are documented in the change control system by the operations department.
D. management has preapproved all emergency changes.

A is the correct answer.

Justification:

A. **Because management cannot always be available when a system failure occurs, it is acceptable for changes to be reviewed and approved within a reasonable time period after they occur.**
B. Although peer review provides some accountability, management should review and approve all changes, even if that review and approval must occur after the fact.
C. Documenting the event does not replace the need for a review and approval process to occur.
D. It is not a good control practice for management to ignore its responsibility by preapproving all emergency changes in advance without reviewing them. Unauthorized changes could then be made without management's knowledge.

A4-195 To optimize an organization's business continuity plan, an IS auditor should recommend a business impact analysis to determine:

A. the business processes that generate the most financial value for the organization and, therefore, must be recovered first.
B. the priorities and order for recovery to ensure alignment with the organization's business strategy.
C. the business processes that must be recovered following a disaster to ensure the organization's survival.
D. the priorities and order of recovery, which will recover the greatest number of systems in the shortest time frame.

C is the correct answer.

Justification:

A. It is a common mistake to overemphasize financial value rather than urgency. For example, while the processing of incoming mortgage loan payments is important from a financial perspective, it could be delayed for a few days in the event of a disaster. On the other hand, wiring funds to close on a loan, while not generating direct revenue, is far more critical because of the possibility of regulatory problems, customer complaints and reputation issues.
B. The business strategy (which is often a long-term view) does not have a direct impact at this point in time.
C. **To ensure the organization's survival following a disaster, it is important to recover the most critical business processes first.**
D. The mere number of recovered systems does not have a direct impact at this point in time. The importance is to recover systems that would impact business survival.

A4-196 Which of the following is the **MOST** efficient strategy for the backup of large quantities of mission-critical data when the systems need to be online to take sales orders 24 hours a day?

A. Implementing a fault-tolerant disk-to-disk backup solution
B. Making a full backup to tape weekly and an incremental backup nightly
C. Creating a duplicate storage area network (SAN) and replicating the data to a second SAN
D. Creating identical server and storage infrastructure at a hot site

A is the correct answer.

Justification:

A. **Disk-to-disk backup, also called disk-to-disk-to-tape backup or tape cache, is when the primary backup is written to disk instead of tape. That backup can then be copied, cloned or migrated to tape at a later time (hence the term "disk-to-disk-to-tape"). This technology allows the backup of data to be performed without impacting system performance and allows a large quantity of data to be backed up in a very short backup window. In case of a failure, the fault-tolerant system can transfer immediately to the other disk set.**
B. While a backup strategy involving tape drives is valid, because many computer systems must be taken offline so that backups can be performed, there is the need to create a backup window, typically during each night. This would not enable the system to be available 24/7. For a system that must remain online at all times, the only feasible way to back up the data is to either duplicate the data to a server that gets backed up to tape, or deploy a disk-to-disk solution, which is effectively the same thing.
C. While creating a duplicate storage area network (SAN) and replicating the data to a second SAN provides some redundancy and data protection, this is not really a backup solution. If the two systems are at the same site, there is a risk that an incident such as a fire or flood in the data center could lead to data loss.
D. While creating an identical server and storage infrastructure at a hot site provides a great deal of redundancy and availability to enable the system to stay operational, it does not address the need for long-term data storage. There is still the need to create an efficient method of backing up data.

A4-197 Which of the following would **BEST** ensure uninterrupted operations in an organization with IT operation centers in several countries?

A. Distribution of key procedural documentation
B. Reciprocal agreement between business partners
C. Strong senior management leadership
D. Employee training on the business continuity plan

D is the correct answer.

Justification:

A. Procedural documentation should always be up to date and distributed to major locations. However, documents alone are insufficient if employees do not know their role in the plan.
B. A reciprocal agreement is an emergency processing agreement between two or more enterprises with similar equipment or applications. Typically, participants of a reciprocal agreement promise to provide processing time to each other when an emergency arises. While it is integral to business continuity to have a location for business operations, it does not necessarily need to be a reciprocal agreement. For example, in some cases, business operations may be carried out from each employee's home.
C. Senior management may not be readily available to provide leadership during a disaster. Therefore, it is most important that employees fully understand their roles in the business continuity plan (BCP).
D. During a disaster, the chain of command might be interrupted. Therefore, it is important that employees know their roles in the BCP, including where to report and how to perform their job functions. Employee training on the plan is especially important for businesses with offices that are geographically separated because there is a greater chance of communication disruption.

A4-198 Which of the following **BEST** ensures that users have uninterrupted access to a critical, heavily used web-based application?

A. Disk mirroring
B. Redundant Array of Inexpensive Disks
C. Dynamic domain name system
D. Load balancing

D is the correct answer.

Justification:

A. Disk mirroring provides real-time replication of disk drives but does not ensure uninterrupted system availability in the event a server crashes.
B. Redundant Array of Inexpensive Disks technology improves resiliency but does not protect against failure of a network interface card or central processing unit processor failure.
C. Dynamic domain name system is a method used to assign a host name to an Internet Protocol address that is dynamic. This is a useful technology but does not help ensure availability.
D. Load balancing best ensures uninterrupted system availability by distributing traffic across multiple servers. Load balancing helps ensure consistent response time for web applications. Also, if a web server fails, load balancing ensures that traffic will be directed to a different, functional server.

A4-199 Which of the following is the **BEST** method to ensure that critical IT system failures do not recur?

A. Invest in redundant systems.
B. Conduct a follow-up audit.
C. Monitor system performance.
D. Perform root cause analysis.

D is the correct answer.

Justification:

A. Redundancy may be a solution; however, a root cause analysis enables an educated decision to address the origin of the problem instead of simply assuming that system redundancy is the solution.
B. While an audit may discover the root cause of the problem, an audit is not a solution to an operational problem. Identifying the origins of operational failures needs to be part of day-to-day IT processes and owned by the IT department.
C. Use of monitoring tools is a means to gather data and can contribute to root cause analysis, but it does not by itself help prevent an existing problem from recurring.
D. Root cause analysis determines the key reason an incident has occurred and allows for appropriate corrections that will help prevent the incident from recurring.

A4-200 Which of the following is **MOST** important when an operating system patch is to be applied to a production environment?

A. Successful regression testing by the developer
B. Approval from the information asset owner
C. Approval from the security officer
D. Patch installation at alternate sites

B is the correct answer.

Justification:

A. While testing is important for any patch, in this case it should be assumed that the operating system (OS) vendor tested the patch before releasing it. Before this OS patch is put into production, the organization should do system testing to ensure that no issues will occur.
B. It is most important that information owners approve any changes to production systems to ensure that no serious business disruption takes place as the result of the patch release.
C. The security officer does not normally need to approve every OS patch.
D. Security patches need to be deployed consistently across the organization, including alternate sites. However, approval from the information asset owner is still the most important consideration.

A4-201 The IS auditor observes that the latest security-related software patches for a mission-critical system were released two months ago, but IT personnel have not yet installed the patches. The IS auditor should:

A. review the patch management policy and determine the risk associated with this condition.
B. recommend that IT systems personnel test and then install the patches immediately.
C. recommend that patches be applied every month or immediately upon release.
D. take no action, because the IT processes related to patch management appear to be adequate.

A is the correct answer.

Justification:

A. **Reviewing the patch management policy and determining whether the IT department is compliant with the policies will detect whether the policies are appropriate and what risk is associated with current practices.**
B. While there may be instances in which the patch is an urgent fix for a serious security issue, IT may have made the determination that the risk to system stability is greater than the risk identified by the software vendor who issued the patch. Therefore, the time frame selected by IT may be appropriate.
C. While keeping critical systems properly patched helps to ensure that they are secure, the requirement for a precise timetable to patch systems may create other issues if patches are improperly tested prior to implementation. Therefore, this is not the correct answer.
D. Even if the IS auditor concludes that the patch management process is adequate, the observation related to the time delay in applying patches should be reported.

A4-202 Which of the following **BEST** helps prioritize the recovery of IT assets when planning for a disaster?

A. Incident response plan
B. Business impact analysis
C. Threat and risk analysis
D. Recovery time objective

B is the correct answer.

Justification:

A. An incident response plan is an organized approach to addressing and managing a security breach or attack. The plan defines what constitutes an incident and the process to follow when an incident occurs. It does not prioritize recovery during a disaster.
B. **Incorporating the business impact analysis (BIA) into the IT disaster recovery planning process is critical to ensure that IT assets are prioritized to align with the business.**
C. Identifying threats and analyzing risk to the business is an important part of disaster planning, but it does not determine the priority of recovery.
D. The recovery time objective is the amount of time allowed for the recovery of a business function or resource after a disaster occurs. This is included as part of the BIA and used to represent the prioritization of recovery.

A4-203 Which of the following is the **MOST** likely reason an organization implements an emergency change to an application using the emergency change control process?

A. The application owner requested new functionality.
B. Changes are developed using an agile methodology.
C. There is a high probability of a significant impact on operations.
D. The operating system vendor has released a security patch.

C is the correct answer.

Justification:

A. Requests for new functionality by the application owner generally follow normal change control procedures, unless they have an impact on the business function.
B. The agile system development methodology breaks down projects into short time-boxed iterations. Each iteration focuses on developing end-to-end functionality from user interface to data storage for the intended architecture. However, the release does not need to follow emergency release procedures unless there is a significant impact on operations.
C. Emergency releases to an application are fixes that require implementation as quickly as possible to prevent significant user downtime. Emergency release procedures are followed in such situations.
D. Operating system security patches are applied after testing, and therefore there is no need for an emergency release.

A4-204 A company with a limited budget has a recovery time objective of 72 hours and a recovery point objective of 24 hours. Which of the following would **BEST** meet the requirements of the business?

A. A hot site
B. A cold site
C. A mirrored site
D. A warm site

D is the correct answer.

Justification:

A. Although a hot site enables the business to meet its recovery point objective (RPO) and recovery time objective (RTO), the cost to maintain a hot site is more than the cost to maintain a warm site, which could also meet the objectives.
B. A cold site, although providing basic infrastructure, lacks the required hardware to meet the business objectives.
C. A mirrored site provides fully redundant facilities with real-time data replication. It can meet the business objectives, but it is not as cost-effective a solution as a warm site.
D. A warm site is the most appropriate solution because it provides basic infrastructure and most of the required IT equipment to affordably meet the business requirements. The remainder of the equipment needed can be provided through vendor agreements within a few days. The RTO is the amount of time allowed for the recovery of a business function or resource after a disaster occurs. The RPO is determined based on the acceptable data loss in case of a disruption of operations. The RPO indicates the earliest point in time that is acceptable to recover the data, and it effectively quantifies the permissible amount of data loss in case of interruption.

A4-205 Which of the following is **MOST** important to determine the recovery point objective for a critical process in an enterprise?

A. Number of hours of acceptable downtime
B. Total cost of recovering critical systems
C. Extent of data loss that is acceptable
D. Acceptable reduction in the level of service

C is the correct answer.

Justification:

A. The recovery time objective is the amount of time allowed for the recovery of a business function or resource after a disaster.
B. The determination of the recovery point objective (RPO) already takes cost into consideration.
C. **The RPO is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the permissible amount of data loss in case of interruption.**
D. The service delivery objective (SDO) is directly related to the business needs. The SDO is the level of services to be reached during the alternate process mode until the normal situation is restored.

A4-206 An IS auditor is assisting in the design of the emergency change control procedures for an organization with a limited budget. Which of the following recommendations **BEST** helps to establish accountability for the system support personnel?

A. Production access is granted to the individual support ID when needed.
B. Developers use a firefighter ID to promote code to production.
C. A dedicated user promotes emergency changes to production.
D. Emergency changes are authorized prior to promotion.

A is the correct answer.

Justification:

A. **Production access should be controlled and monitored to ensure segregation of duties. During an emergency change, a user who normally does not have access to production may require access. The best process to ensure accountability within the production system is to have the information security team create a production support group and add the user ID to that group to promote the change. When the change is complete the ID can be removed from the group. This process ensures that activity in production is linked to the specific ID that was used to make the change.**
B. Some organizations may use a firefighter ID, which is a generic/shared ID, to promote changes to production. When needed, the developer can use this ID to access production. It may still be difficult to determine who made the change; therefore, although this process is commonly used, the use of a production support ID is a better choice.
C. Having a dedicated user who promotes changes to production in an emergency is ideal but is generally not cost-effective and may not be realistic for emergency changes.
D. Emergency changes are, by definition, unauthorized changes. Approvals usually are obtained following promotion of the change to production. All changes should be auditable, and that can best be accomplished by having a user ID added/removed to the production support group as needed.

A4-207 Segmenting a highly sensitive database results in:

A. reduced exposure.
B. reduced threat.
C. less criticality.
D. less sensitivity.

A is the correct answer.

Justification:
A. Segmenting data reduces the quantity of data exposed to a particular vulnerability.
B. The threat may remain constant, but each segment represents a different vector against which it must be directed.
C. Criticality is a data attribute and is not affected by the manner in which it is segmented.
D. Sensitivity is a data attribute and is not affected by the manner in which it is segmented.

A4-208 Which of the following is the **BEST** way to ensure that incident response activities are consistent with the requirements of business continuity?

A. Draft and publish a clear practice for enterprise-level incident response.
B. Establish a cross-departmental working group to share perspectives.
C. Develop a scenario and perform a structured walk-through.
D. Develop a project plan for end-to-end testing of disaster recovery.

C is the correct answer.

Justification:
A. Publishing an enterprise-level incident response plan is effective only if business continuity aligned itself to incident response. Incident response supports business continuity, not the other way around.
B. Sharing perspectives is valuable, but a working group does not necessarily lead to ensuring that the interface between plans is workable.
C. A structured walk-through including both incident response and business continuity personnel provides the best opportunity to identify gaps or misalignments between the plans.
D. A project plan developed for disaster recovery will not necessarily address deficiencies in business continuity or incident response.

A4-209 An IS auditor is evaluating network performance for an organization that is considering increasing its Internet bandwidth due to a performance degradation during business hours. Which of the following is **MOST** likely the cause of the performance degradation?

A. Malware on servers
B. Firewall misconfiguration
C. Increased spam received by the email server
D. Unauthorized network activities

D is the correct answer.

Justification:

A. The existence of malware on the organization's server could contribute to network performance issues, but the degraded performance would not likely be restricted to business hours.
B. Firewall misconfiguration could contribute to network performance issues, but the degraded performance would not likely be restricted to business hours.
C. The existence of spam on the organization's email server could contribute to network performance issues, but the degraded performance would not likely be restricted to business hours.
D. Unauthorized network activities—such as employee use of file or music sharing sites or online gambling or personal email containing large files or photos—could contribute to network performance issues. Because the IS auditor found the degraded performance during business hours, this is the most likely cause.

A4-210 Which of the following is the **BEST** method for an IS auditor to verify that critical production servers are running the latest security updates released by the vendor?

A. Ensure that automatic updates are enabled on critical production servers.
B. Verify manually that the patches are applied on a sample of production servers.
C. Review the change management log for critical production servers.
D. Run an automated tool to verify the security patches on production servers.

D is the correct answer.

Justification:

A. Ensuring that automatic updates are enabled on production servers may be a valid way to manage the patching process; however, this would not provide assurance that all servers are being patched appropriately.
B. Verifying patches manually on a sample of production servers will be less effective than automated testing and introduces a significant audit risk. Manual testing is also difficult and time consuming.
C. The change management log may not be updated on time and may not accurately reflect the patch update status on servers. A better testing strategy is to test the server for patches, rather than examining the change management log.
D. An automated tool can immediately provide a report on which patches have been applied and which are missing.

A4-211 An IS auditor is conducting a review of the disaster recovery procedures for a data center. Which of the following indicators **BEST** shows that the procedures meet the requirements?

A. Documented procedures were approved by management.
B. Procedures were reviewed and compared with industry good practices.
C. A tabletop exercise using the procedures was conducted.
D. Recovery teams and their responsibilities are documented.

C is the correct answer.

Justification:

A. Management approval does not necessarily mean that the disaster recovery procedures are sufficient to meet the needs of the business.
B. While it is useful to compare the procedures with documented industry good practices, a tabletop exercise (paper test) is a better indicator that the procedures meet requirements.
C. **Conducting a tabletop exercise (paper-based test) of the procedures with all responsible members, best ensures that the procedures meet the requirements. This type of test can identify missing or incorrect procedures because representatives responsible for performing the tasks are present.**
D. The documentation of recovery teams and their responsibilities would be part of the procedures and not necessarily validate that the procedures are correct and complete thus meeting requirements.

A4-212 Which of the following choices **BEST** ensures accountability when updating data directly in a production database?

A. Review of audit logs
B. Principle of least privilege
C. Approved validation plan
D. Segregation of duties

A is the correct answer.

Justification:

A. **Detailed audit logs that contain the user ID of the individual who performed the change as well as the data before and after the change are the best evidence of database changes. A review of these logs would evidence the individual who changed the data (ensuring accountability) as well as the correctness of the change.**
B. Although access to production databases should be controlled by the principle of least privilege, this does not evidence who made the change or if the change was made correctly.
C. Having an approved validation plan evidences that the change was made correctly but does not show who made the change in production. Only a system-generated audit log can prove accountability.
D. Segregation of duties only ensures that the user making the data change is different than the individual who approved the data change. It would not evidence the individual who made the change, nor would it ensure that the data change was correct.

A4-213 An IS auditor has discovered that a new patch is available for an application, but the IT department has decided that the patch is not needed because other security controls are in place. What should the IS auditor recommend?

A. Apply the patch only after it has been thoroughly tested.
B. Implement a host-based intrusion detection system.
C. Modify the firewall rules to further protect the application server.
D. Assess the overall risk, then recommend whether to deploy the patch.

D is the correct answer.

Justification:

A. Applying a patch without first performing a risk assessment might be a waste of resources if it is determined that the application is not mission critical.
B. Implementing a host-based intrusion detection system would be a valid control; however, it may not address vulnerabilities within the application.
C. Modifying the firewall rules may help to mitigate the risk of a security incident; however, first the risk related to the patch would need to be determined.
D. While it is important to ensure that systems are properly patched, a risk assessment needs to be performed to determine the likelihood and probability of the vulnerability being exploited. Therefore, the patch would be applied only if the risk of circumventing the existing security controls is great enough to warrant it.

A4-214 An IS auditor is reviewing the most recent disaster recovery plan of an organization. Which approval is the **MOST** important when determining the availability of system resources required for the plan?

A. Executive management
B. IT management
C. Board of directors
D. Steering committee

B is the correct answer.

Justification:

A. Although executive management's approval is essential, the IT department is responsible for managing system resources and their availability as related to disaster recovery (DR).
B. Because a disaster recovery plan (DRP) is based on the recovery and provisioning of IT services, IT management's approval would be most important to verify that the system resources will be available in the event that a disaster event is triggered.
C. The board of directors may review and approve the DRP, but the IT department is responsible for managing system resources and their availability as related to DR.
D. The steering committee would determine the requirements for disaster recovery (recovery time objective and recovery point objective); however, the IT department is responsible for managing system resources and their availability as related to DR.

A4-215 Which of the following inputs would **PRIMARILY** help in designing the data backup strategy in case of potential natural disasters?

A. Recovery point objective
B. Volume of data to be backed up
C. Available data backup technologies
D. Recovery time objective

A is the correct answer.

Justification:

A. **The recovery point objective (RPO) is determined based on the acceptable data loss in case of a disruption of operations. It indicates the earliest point in time that is acceptable to recover the data. The RPO effectively quantifies the acceptable amount of data loss in the case of interruption. Based on the RPO, one can design the data backup strategy for potential disasters using various technologies.**
B. While the amount of data to be stored is critical in terms of planning for adequate capacity, the speed of recovery required by the business is the most important factor.
C. While a solid understanding of the capabilities of all types of advanced data backup technologies is necessary, without the knowledge of the RPO one cannot design a backup strategy using these technologies.
D. The recovery time objective is the amount of time allowed for the recovery of a business function or resource after a disaster occurs. This will help in designing disaster site options, but not the data backup strategy in the case of impacting disasters.

A4-216 While conducting an audit on the customer relationship management application, the IS auditor observes that it takes a significantly long time for users to log on to the system during peak business hours as compared with other times of the day. Once logged on, the average response time for the system is within acceptable limits. Which of the following choices should the IS auditor recommend?

A. No action should be taken because the system meets current business requirements.
B. IT should increase the network bandwidth to improve performance.
C. Users should be provided with detailed manuals to use the system properly.
D. Establish performance measurement criteria for the authentication servers.

D is the correct answer.

Justification:

A. The IS auditor should not recommend taking no action because a delayed login process has a negative impact on employee productivity.
B. Network bandwidth may or may not be the root cause of this issue. Performance measurement criteria may help determine the cause, which can then be remediated.
C. Because the problem is related to logging on and not to processing, additional training for users would not be effective in this case.
D. **Performance criteria for the authentication servers would help to quantify acceptable thresholds for system performance, which can be measured and remediated.**

A4-217 Due to resource constraints, a developer requires full access to production data to support certain problems reported by production users. Which of the following choices would be a good compensating control for controlling unauthorized changes in production?

A. Provide and monitor separate developer login IDs for programming and for production support.
B. Capture activities of the developer in the production environment by enabling detailed audit trails.
C. Back up all affected records before allowing the developer to make production changes.
D. Ensure that all changes are approved by the change manager prior to implementation.

A is the correct answer.

Justification:

A. Providing separate login IDs that would only allow a developer privileged access when required is a good compensating control, but it must also be backed up with monitoring and supervision of the activity of the developer.
B. While capturing activities of the developer via audit trails or logs would be a good practice, the control would not be effective unless these audit trails are reviewed on a periodic basis.
C. Creating a backup of affected records before making the change would allow for rollback in case of an error but would not prevent or detect unauthorized changes.
D. Even though changes are approved by the change manager, a developer with full access can easily circumvent this control.

A4-218 Which of the following choices would **MOST** likely ensure that a disaster recovery effort is successful?

A. The tabletop test was performed.
B. Data restoration was completed.
C. Recovery procedures are approved.
D. Appropriate staff resources are committed.

B is the correct answer.

Justification:

A. Performing a tabletop test is extremely helpful but does not ensure that the recovery process is working properly.
B. The most reliable method to determine whether a backup is valid would be to restore it to a system. A data restore test should be performed at least annually to verify that the process is working properly.
C. Approved recovery procedures will not ensure that data can be successfully restored.
D. While having appropriate staff resources is appropriate, without data the recovery would not be successful.

A4-219 An IS auditor is auditing an IT disaster recovery plan. The IS auditor should **PRIMARILY** ensure that the plan covers:

A. a resilient IT infrastructure.
B. alternate site information.
C. documented disaster recovery test results.
D. analysis and prioritization of business functions.

D is the correct answer.

Justification:

A. A resilient IT infrastructure is typically required to minimize interruptions to IT services; however, if a critical business function does not require high availability of IT, this may not be required for all disaster recovery plan (DRP) elements.
B. While the selection of an alternate site is important, the more critical issue is the prioritization of resources based on impact and recovery time objectives (RTOs) of business functions.
C. Documented DRP test results are helpful when maintaining the DRP; however, the DRP must first and foremost be aligned with business requirements.
D. The DRP must primarily focus on recovering critical business functions in the event of disaster within predefined RTOs; thus, it is necessary to align the recovery of IT services based on the criticality of business functions.

A4-220 An IS auditor observed that users are occasionally granted the authority to change system data. This elevated system access yet is required for smooth functioning of business operations. Which of the following controls would the IS auditor **MOST** likely recommend for long-term resolution?

A. Redesign the controls related to data authorization.
B. Implement additional segregation of duties controls.
C. Review policy to see if a formal exception process is required.
D. Implement additional logging controls.

C is the correct answer.

Justification:

A. Data authorization controls should be driven by the policy. While there may be some technical controls that could be adjusted, if the data changes happen infrequently, then an exception process would be the better choice.
B. While adequate segregation of duties is important, the IS auditor must first review policy to see if there is a formal documented process for this type of temporary access controls to enforce segregation of duties.
C. If the users are granted access to change data in support of the business requirements, and the policy should be followed. If there is no policy for the granting of extraordinary access, then one should be designed to ensure no unauthorized changes are made.
D. Audit trails are needed whenever temporary elevated access is required. However, but this is not the first step the auditor should take in reviewing the overall process.

A4-221 A medium-sized organization, whose IT disaster recovery measures have been in place and regularly tested for years, has just developed a formal business continuity plan (BCP). A basic BCP tabletop exercise has been performed successfully. Which testing should an IS auditor recommend be performed next to verify the adequacy of the new BCP?

A. Full-scale test with relocation of all departments, including IT, to the contingency site
B. Walk-through test of a series of predefined scenarios with all critical personnel involved
C. IT disaster recovery test with business departments involved in testing the critical applications
D. Functional test of a scenario with limited IT involvement

D is the correct answer.

Justification:

A. A full-scale test in the situation described might fail because it would be the first time that the plan is actually exercised, and a number of resources (including IT) and time would be wasted.
B. The walk-through test is a basic type of testing. Its intention is to make key staff familiar with the plan and discuss critical plan elements, rather than verifying its adequacy.
C. The recovery of applications should always be verified and approved by the business instead of being purely IT-driven. The IT plan has been tested repeatedly so a disaster recovery test would not help in verifying the administrative and organizational parts of the BCP, which are not IT-related.
D. After a tabletop exercise has been performed, the next step would be a functional test, which includes the mobilization of staff to exercise the administrative and organizational functions of a recovery. Because the IT part of the recovery has been tested for years, it would be more efficient to verify and optimize the BCP before actually involving IT in a full-scale test. The full-scale test would be the last step of the verification process before entering into a regular annual testing schedule.

A4-222 Which of the following business continuity plan tests involves participation of relevant members of the crisis management/response team to practice proper coordination?

A. Tabletop
B. Functional
C. Full-scale
D. Deskcheck

A is the correct answer.

Justification:

A. The primary purpose of tabletop testing is to practice proper coordination because it involves all or some of the crisis team members and is focused more on coordination and communication issues than on technical process details.
B. Functional testing involves mobilization of personnel and resources at various geographic sites. This is a more in-depth functional test and not primarily focused on coordination and communication.
C. Full-scale testing involves enterprisewide participation and full involvement of external organizations.
D. Deskcheck testing requires the least effort of the options given. Its aim is to ensure the plan is up to date and promote familiarity of the BCP to critical personnel from all areas.

A4-223 Which of the following is the **BEST** method to ensure that the business continuity plan remains up to date?

A. The group walks through the different scenarios of the plan from beginning to end.
B. The group ensures that specific systems can actually perform adequately at the alternate offsite facility.
C. The group is aware of full-interruption test procedures.
D. Interdepartmental communication is promoted to better respond in the case of a disaster.

A is the correct answer.

Justification:

A. A structured walk-through test gathers representatives from each department who will review the plan and identify weaknesses.
B. The ability of the group to ensure that specific systems can actually perform adequately at the alternate offsite facility is a parallel test and does not involve group meetings.
C. Group awareness of full-interruption test procedures is the most intrusive test to regular operations and the business.
D. While improving communication is important, it is not the most valued method to ensure that the plan is up to date.

A4-224 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?

A. Full operational test
B. Preparedness test
C. Paper test
D. Regression test

B is the correct answer.

Justification:

A. A full operational test is conducted after the paper and preparedness test and is quite expensive.
B. A preparedness test is performed by each local office/area to test the adequacy of the preparedness of local operations for disaster recovery.
C. A paper test is a structured walk-through of the disaster recovery plan and should be conducted before a preparedness test, but a paper test (deskcheck) is not sufficient to test the viability of the plan.
D. A regression test is not a disaster recovery plan test and is used in software development and maintenance.

A4-225 An organization's disaster recovery plan should address early recovery of:

A. all information systems processes.
B. all financial processing applications.
C. only those applications designated by the IS manager.
D. processing in priority order, as defined by business management.

D is the correct answer.

Justification:

A. A disaster recovery plan (DRP) will recover most critical systems first according to business priorities.
B. Depending on business priorities, financial systems may or may not be the first to be recovered.
C. The business manager, not the IS manager, will determine priorities for system recovery.
D. Business management should know which systems are critical and what they need to process well in advance of a disaster. It is management's responsibility to develop and maintain the plan. Adequate time will not be available for this determination once the disaster occurs. IS and the information processing facility are service organizations that exist for the purpose of assisting the general user management in successfully performing their jobs.

A4-226 Disaster recovery planning addresses the:

A. technological aspect of business continuity planning (BCP).
B. operational part of BCP.
C. functional aspect of BCP.
D. overall coordination of BCP.

A is the correct answer.

Justification:

A. Disaster recovery planning (DRP) is the technological aspect of business continuity planning (BCP) that focuses on IT systems and operations.
B. Business resumption planning addresses the operational part of BCP.
C. Disaster recovery addresses the technical components of business recovery.
D. The overall coordination of BCP is accomplished through business continuity management and strategic plans. DRP addresses technical aspects of BCP.

A4-227 Which of the following must exist to ensure the viability of a duplicate information processing facility?

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

C is the correct answer.

Justification:

A. The site chosen should not be subject to the same natural disaster as the primary site. Being close may be a risk or an advantage, depending on the type of expected disaster.
B. A reasonable compatibility of hardware/software must exist to serve as a basis for backup. The latest or newest hardware may not adequately serve this need.
C. Resource availability must be assured. The workload of the primary site must be monitored to ensure that availability at the alternate site for emergency backup use is sufficient.
D. Testing the hardware when the site is established is essential, but regular testing of the actual backup data is necessary to ensure that the operation will continue to perform as planned.

A4-228 The cost of ongoing operations when a disaster recovery plan (DRP) is in place, compared to not having a DRP, will **MOST** likely:

A. increase.
B. decrease.
C. remain the same.
D. be unpredictable.

A is the correct answer.

Justification:

A. Due to the additional cost of testing, maintaining and implementing disaster recovery plan (DRP) measures, the cost of normal operations for any organization will always increase after a DRP implementation (i.e., the cost of normal operations during a nondisaster period will be more than the cost of operations during a nondisaster period when no DRP was in place).
B. The implementation of a DRP will always result in additional costs to the organization.
C. The implementation of a DRP will always result in additional costs to the organization.
D. The costs of a DRP are fairly predictable and consistent.

A4-229 Which of the following tasks should be performed **FIRST** when preparing a disaster recovery plan?

A. Develop a recovery strategy
B. Perform a business impact analysis
C. Map software systems, hardware and network components
D. Appoint recovery teams with defined personnel, roles and hierarchy

B is the correct answer.

Justification:
A. Developing a recovery strategy will come after performing a business impact analysis (BIA).
B. The first step in any disaster recovery plan is to perform a BIA.
C. The BIA will identify critical business processes and the systems that support those processes. Mapping software systems, hardware and network components will come after performing a BIA.
D. Appointing recovery teams with defined personnel, roles and hierarchy will come after performing a BIA.

A4-230 After completing the business impact analysis, what is the **NEXT** step in the business continuity planning process?

A. Test and maintain the plan.
B. Develop a specific plan.
C. Develop recovery strategies.
D. Implement the plan.

C is the correct answer.

Justification:
A. After selecting a strategy, a specific business continuity plan (BCP) can be developed, tested and implemented.
B. After selecting a strategy, a specific BCP can be developed, tested and implemented.
C. Once the business impact analysis (BIA) is completed, the next phase in the BCP development is to identify the various recovery strategies and select the most appropriate strategy for recovering from a disaster that will meet the time lines and priorities defined through the BIA.
D. After selecting a strategy, a specific BCP can be developed, tested and implemented.

A4-231 Which of the following is an appropriate test method to apply to a business continuity plan?

A. Pilot
B. Paper
C. Unit
D. System

B is the correct answer.

Justification:
A. A pilot test is used for implementing a new process or technology and is not appropriate for a business continuity planning (BCP).
B. A paper test (sometimes called a deskcheck) is appropriate for testing a BCP. It is a walk-through of the entire BCP, or part of the BCP, involving major players in the BCP's execution who reason out what may happen in a particular disaster.
C. A unit test is used to test new software components and is not appropriate for a BCP.
D. A system test is an integrated test used to test a new IT system but is not appropriate for a BCP.

A4-232 As part of the business continuity planning process, which of the following should be identified **FIRST** in the business impact analysis?

A. Risk such as single point-of-failure and infrastructure risk
B. Threats to critical business processes
C. Critical business processes for ascertaining the priority for recovery
D. Resources required for resumption of business

C is the correct answer.

Justification:
A. Risk should be identified after the critical business processes have been identified.
B. The identification of threats to critical business processes can only be determined after the critical business processes have been identified.
C. **The identification of critical business processes should be addressed first so that the priorities and time lines for recovery can be documented.**
D. Identification of resources required for business resumption will occur after the identification of critical business processes.

A4-233 Which of the following would contribute **MOST** to an effective business continuity plan?

A. The document is circulated to all interested parties.
B. Planning involves all user departments.
C. The plan is approved by senior management.
D. An audit is performed by an external IS auditor.

B is the correct answer.

Justification:
A. The business continuity plan (BCP) circulation will ensure that the BCP document is received by all users. Although essential, this does not contribute significantly to the success of the BCP.
B. **The involvement of user departments in the BCP is crucial for the identification of the business processing priorities and the development of an effective plan.**
C. A BCP approved by senior management would not necessarily ensure the effectiveness of the BCP.
D. An audit would not necessarily improve the quality of the BCP.

A4-234 The **PRIMARY** objective of business continuity and disaster recovery plans should be to:

A. safeguard critical IS assets.
B. provide for continuity of operations.
C. minimize the loss to an organization.
D. protect human life.

D is the correct answer.

Justification:
A. Safeguarding critical IS assets is a secondary objective of a business continuity and disaster recovery plan. The first priority is always life safety.
B. Providing continuity of operations is a secondary objective of a business continuity and disaster recovery plan. The first priority is always life safety.
C. Minimizing the loss to an organization is a secondary objective of a business continuity and disaster recovery plan. The first priority is always life safety.
D. **Because human life is invaluable, the main priority of any business continuity and disaster recovery plan should be to protect people.**

A4-235 Depending on the complexity of an organization's business continuity plan (BCP), it may be developed as a set of plans to address various aspects of business continuity and disaster recovery. In such an environment, it is essential that:

A. each plan is consistent with one another.
B. all plans are integrated into a single plan.
C. each plan is dependent on one another.
D. the sequence for implementation of all plans is defined.

A is the correct answer.

Justification:

A. **Depending on the complexity of an organization, there could be more than one plan to address various aspects of business continuity and disaster recovery, but the plans must be consistent to be effective.**
B. The plans do not necessarily have to be integrated into one single plan.
C. Although each plan may be independent, each plan has to be consistent with other plans to have a viable business continuity planning strategy.
D. It may not be possible to define a sequence in which plans have to be implemented because it may be dependent on the nature of disaster, criticality, recovery time, etc.

A4-236 When developing a business continuity plan, which of the following tools should be used to gain an understanding of the organization's business processes?

A. Business continuity self-audit
B. Resource recovery analysis
C. Risk assessment
D. Gap analysis

C is the correct answer.

Justification:

A. Business continuity self-audit is a tool for evaluating the adequacy of the business continuity plan (BCP) but not for gaining an understanding of the business.
B. Resource recovery analysis is a tool for identifying the components necessary for a business resumption strategy but not for gaining an understanding of the business.
C. **Risk assessment and business impact assessment are tools for understanding the business as a part of BCP.**
D. The role gap analysis can play in BCP is to identify deficiencies in a plan but not for gaining an understanding of the business.

A4-237 Which of the following should be of **MOST** concern to an IS auditor reviewing the business continuity plan (BCP)?

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

D is the correct answer.

Justification:

A. Although failure to consider duration could be a problem, it is not as significant as scope, and neither is as critical as the need to identify someone with the authority to invoke the business continuity plan (BCP).
B. The difference between incidents and low-level disasters is always unclear and frequently revolves around the amount of time required to correct the damage.
C. The lack of detailed steps should be documented, but their absence does not mean a lack of recovery if, in fact, someone has invoked the BCP.
D. If nobody declares the disaster, the BCP would not be invoked, making all other concerns less important.

A4-238 During an audit of a business continuity plan (BCP), an IS auditor found that, although all departments were housed in the same building, each department had a separate BCP. The IS auditor recommended that the BCPs be reconciled. Which of the following areas should be reconciled **FIRST**?

A. Evacuation plan
B. Recovery priorities
C. Backup storages
D. Call tree

A is the correct answer.

Justification:

A. Protecting human resources during a disaster-related event should be addressed first. Having separate business continuity plans could result in conflicting evacuation plans, thus jeopardizing the safety of staff and clients.
B. Recovery priorities may be unique to each department and could be addressed separately, but still should be reviewed for possible conflicts and/or the possibility of cost reduction, but only after the issue of human safety has been analyzed.
C. Backup strategies are not critical to the integration of the plans for the various departments. Life safety is always the first priority.
D. Communication during a crisis is always a challenge, but the call tree is not as important as ensuring life safety first.

A4-239 For effective implementation after a business continuity plan (BCP) has been developed, it is **MOST** important that the BCP be:

A. stored in a secure, offsite facility.
B. approved by senior management.
C. communicated to appropriate personnel.
D. made available through the enterprise's intranet.

C is the correct answer.

Justification:
A. The business continuity plan (BCP), if kept in a safe place, will not reach the users; users will never implement the BCP and, thus, the BCP will be ineffective.
B. Senior management approval is a prerequisite for designing and approving the BCP but is less important than making sure that the plan is available to all key personnel to ensure that the plan will be effective.
C. The implementation of a BCP will be effective only if appropriate personnel are informed and aware of all the aspects of the BCP.
D. Making a BCP available on an enterprise's intranet does not guarantee that personnel will be able to access, read or understand it.

A4-240 Which of the following is the **PRIMARY** objective of the business continuity plan process?

A. To provide assurance to stakeholders that business operations will continue in the event of disaster
B. To establish an alternate site for IT services to meet predefined recovery time objectives
C. To manage risk while recovering from an event that adversely affected operations
D. To meet the regulatory compliance requirements in the event of natural disaster

C is the correct answer.

Justification:
A. The business continuity plan (BCP) in itself does not provide assurance of continuing operations; however, it helps the organization to respond to disruptions to critical business processes.
B. Establishment of an alternate site is more relevant to disaster recovery than the BCP.
C. The BCP process primarily focuses on managing and mitigating risk during recovery of operations due to an event that affected operations.
D. The regulatory compliance requirements may help establish the recovery time objective (RTO) requirements.

A4-241 Which of the following would **BEST** help to detect errors in data processing?

A. Programmed edit checks
B. Well-designed data entry screens
C. Segregation of duties
D. Hash totals

D is the correct answer.

Justification:
A. Automated controls such as programmed edit checks are preventive controls.
B. Automated controls such as well-designed data entry screens are preventive controls.
C. Enforcing segregation of duties primarily ensures that a single individual does not have the authority to both create and approve a transaction; this is not considered to be a method to detect errors, but a method to help prevent errors.
D. The use of hash totals is an effective method to reliably detect errors in data processing. A hash total would indicate an error in data integrity.

A4-242 Which of the following is the **MOST** critical to the quality of data in a data warehouse?

A. Accuracy of the source data
B. Credibility of the data source
C. Accuracy of the extraction process
D. Accuracy of the data transformation

A is the correct answer.

Justification:

A. **Accuracy of source data is a prerequisite for the quality of the data in a data warehouse. Inaccurate source data will corrupt the integrity of the data in the data warehouse.**
B. Credibility of the data source is important but would not change inaccurate data into quality (accurate) data.
C. Accurate extraction processes are important but would not change inaccurate data into quality (accurate) data.
D. Accurate transformation routines are important but would not change inaccurate data into quality (accurate) data.

A4-243 A clerk changed the interest rate for a loan on a master file. The rate entered is outside the normal range for such a loan. Which of the following controls is **MOST** effective in providing reasonable assurance that the change was authorized?

A. The system will not process the change until the clerk's manager confirms the change by entering an approval code
B. The system generates a weekly report listing all rate exceptions and the report is reviewed by the clerk's manager
C. The system requires the clerk to enter an approval code
D. The system displays a warning message to the clerk

A is the correct answer.

Justification:

A. **Requiring an approval code by a manager would prevent or detect the use of an unauthorized interest rate.**
B. A weekly report would inform the manager after the fact that a change was made, thereby making it possible for transactions to use an unauthorized rate prior to management review.
C. Having a clerk enter an approval code would not provide separation of duties and would not prevent the clerk from entering an unauthorized rate change.
D. A warning message would alert the clerk in case the change was being made in error but would not prevent the clerk from entering an unauthorized rate change.

A4-244 The **GREATEST** advantage of using web services for the exchange of information between two systems is:

A. Secure communication
B. Improved performance
C. Efficient interfacing
D. Enhanced documentation

C is the correct answer.

Justification:
A. Communication is not necessarily more secure using web services.
B. The use of web services will not necessarily increase performance.
C. **Web services facilitate the interoperable exchange of information between two systems regardless of the operating system or programming language used.**
D. There is no documentation benefit in using web services

A4-245 Which of the following is a prevalent risk in the development of end-user computing applications?

A. Applications may not be subject to testing and IT general controls.
B. Development and maintenance costs may be increased.
C. Application development time may be increased.
D. Decision-making may be impaired due to diminished responsiveness to requests for information.

A is the correct answer.

Justification:
A. **End-user computing (EUC) is defined as the ability of end users to design and implement their own information system using computer software products. End-user developed applications may not be subjected to an independent outside review by systems analysts and frequently are not created in the context of a formal development methodology. These applications may lack appropriate standards, controls, quality assurance procedures, and documentation. A risk of end-user applications is that management may rely on them as much as traditional applications.**
B. EUC systems typically result in reduced application development and maintenance costs.
C. EUC systems typically result in a reduced development cycle time.
D. EUC systems normally increase flexibility and responsiveness to management's information requests because the system is being developed directly by the user community.

A4-246 An IS auditor finds out-of-range data in some tables of a database. Which of the following controls should the IS auditor recommend to avoid this situation?

A. Log all table update transactions
B. Implement integrity constraints in the database
C. Implement before and after image reporting
D. Use tracing and tagging

B is the correct answer.

Justification:
A. Logging all table update transactions provides audit trails and is a detective control but will not prevent the introduction of inaccurate data.
B. **Implementing integrity constraints in the database is a preventive control because data are checked against predefined tables or rules, which prevents any undefined data from being entered.**
C. Before and after image reporting makes it possible to trace the impact that transactions have on computer records and is a detective control.
D. Tracing and tagging is used to test application systems and controls but is not a preventive control that can avoid out-of-range data.

A4-247 A new database is being set up in an overseas location to provide information to the general public and to increase the speed at which the information is made available. The overseas database is to be housed at a data center and will be updated in real time to mirror the information stored locally. Which of the following areas of operations should be considered as having the **HIGHEST** risk?

A. Confidentiality of the information stored in the database
B. The hardware being used to run the database application
C. Backups of the information in the overseas database
D. Remote access to the backup database

B is the correct answer.

Justification:

A. Confidentiality of the information stored in the database is not a major concern, because the information is intended for public use.
B. The business objective is to make the information available to the public in a timely manner. Because the database is physically located overseas, hardware failures that are left unfixed can reduce the availability of the system to users.
C. Backups of the information in the overseas database are not a major concern, because the overseas database is a mirror of the local database; thus, a backup copy exists locally.
D. Remote access to the backup database does not impact availability.

A4-248 Which of the following is the **MOST** effective when determining the correctness of individual account balances migrated from one database to another?

A. Compare the hash total before and after the migration
B. Verify that the number of records is the same for both databases
C. Perform sample testing of the migrated account balances
D. Compare the control totals of all of the transactions

C is the correct answer.

Justification:

A. The hash total will only validate the data integrity at a batch level rather than at a transaction level.
B. Databases are composed of records that can contain multiple fields. The number of records will not allow an IS auditor to ascertain whether some of these fields have been successfully migrated.
C. Performing sample testing of the migrated account balances will involve the comparison of a selection of individual transactions from the database before and after the migration.
D. Comparing the control totals does not imply that the records are complete or that individual values are accurate.

A4-249 During the review of data file change management controls, which of the following **BEST** helps to decrease the research time needed to investigate exceptions?

A. One-for-one checking
B. Data file security
C. Transaction logs
D. File updating and maintenance authorization

C is the correct answer.

Justification:

A. One-for-one checking is a control procedure in which an individual document agrees with a detailed listing of documents processed by the system. It would take a long time to complete the research using this procedure.
B. Data file security controls prevent access by unauthorized users in their attempt to alter data files. This would not help identify the transactions posted to an account.
C. **Transaction logs generate an audit trail by providing a detailed list of date of input, time of input, user ID, terminal location, etc. Research time can be reduced in investigating exceptions because the review can be performed on the logs rather than on the entire transaction file. It also helps to determine which transactions have been posted to an account—by a particular individual during a particular period.**
D. File updating and maintenance authorization is a control procedure to update the stored data and ensure accuracy and security of stored data. This does provide evidence regarding the individuals who update the stored data; however, it is not effective in the given situation to determine transactions posted to an account.

A4-250 An IS auditor is reviewing a monthly accounts payable transaction register using audit software. For what purpose would the auditor be interested in using a check digit?

A. To detect data transposition errors
B. To ensure that transactions do not exceed predetermined amounts
C. To ensure that data entered are within reasonable limits
D. To ensure that data entered are within a predetermined range of values

A is the correct answer.

Justification:

A. **A check digit is a numeric value added to data to ensure that original data are correct and have not been altered.**
B. Ensuring that data have not exceeded a predetermined amount is a limit check.
C. Ensuring that data entered are within predetermined reasonable limits is a reasonableness check.
D. Ensuring that data entered are within a predetermined range of values is a range check.

A4-251 A hard disk containing confidential data was damaged beyond repair. If the goal is to positively prevent access to the data by anyone else, what should be done to the hard disk before it is discarded?

A. Overwriting
B. Low-level formatting
C. Degaussing
D. Destruction

D is the correct answer.

Justification:
A. Rewriting data is impractical because the hard disk is damaged and offers less assurance than physical destruction even when done successfully.
B. Low-level formatting is impractical because the hard disk is damaged and offers less assurance than physical destruction even when done successfully.
C. Degaussing is highly effective but offers less assurance than physical destruction.
D. Physically destroying the hard disk is the most effective way to ensure that data cannot be recovered.

A4-252 Authorizing access to application data is the responsibility of the:

A. data custodian.
B. application administrator.
C. data owner.
D. security administrator.

C is the correct answer.

Justification:
A. Data custodians are responsible only for storing and safeguarding the data according to the direction provided by the data owner.
B. An application administrator is responsible for managing the application itself, not determining who is authorized to access the data that it contains.
C. Data owners have authority to grant or withhold access to the data and applications for which they are responsible.
D. The security administrator may lead investigations and is responsible for implementing and maintaining information security policy, but not for authorizing data access.

A4-253 An IS auditor finds that a database administrator (DBA) has read and write access to production data. The IS auditor should:

A. accept the DBA access as a common practice.
B. assess the controls relevant to the DBA function.
C. recommend the immediate revocation of the DBA access to production data.
D. review user access authorizations approved by the DBA.

B is the correct answer.

Justification:
A. Although granting access to production data to the database administrator (DBA) may be a common practice, the IS auditor should evaluate the relevant controls.
B. When reviewing privileged accounts, the auditor should look for compensating controls that may address a potential exposure.
C. The DBA should have access based on the principle of least privilege; unless care is taken to validate what access is required, revocation may remove access the DBA requires to do his/her job.
D. Granting user authorizations is the responsibility of the data owner, not the DBA, and access to production data is not generally associated with user access authorizations.

A4-254 Which of the following is the **MOST** effective method for disposing of magnetic media that contains confidential information?

A. Degaussing
B. Defragmenting
C. Erasing
D. Destroying

D is the correct answer.

Justification:

A. Degaussing or demagnetizing is a good control, but not sufficient to fully erase highly confidential information from magnetic media.
B. The purpose of defragmentation is to improve efficiency by eliminating fragmentation in file systems; it does not remove information.
C. Erasing or deleting magnetic media does not remove the information; this method simply changes a file's indexing information.
D. Destroying magnetic media is the only way to assure that confidential information cannot be recovered.

A4-255 Which of the following should an IS auditor recommend for the protection of specific sensitive information stored in a data warehouse?

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

A is the correct answer.

Justification:

A. Column- and row-level permissions control what information users can access. Column-level security prevents users from seeing one or more attributes on a table. With row-level security a certain grouping of information on a table is restricted (e.g., if a table held details of employee salaries, then a restriction could be put in place to ensure that, unless specifically authorized, users could not view the salaries of executive staff). Column- and row-level security can be achieved in a relational database by allowing users to access logical representations of data (views) rather than physical tables. This "fine-grained" security model is likely to offer the best balance between information protection while still supporting a wide range of analytical and reporting uses.
B. Enhancing user authentication via strong passwords is a security control that should apply to all users of the data warehouse and does not specifically address protection of specific sensitive data.
C. Organizing a data warehouse into subject-specific databases is a potentially useful practice but, in itself, does not adequately protect sensitive data. Database-level security is normally too "coarse" a level to efficiently and effectively protect information. For example, one database may hold information that needs to be restricted such as employee salary and customer profitability details while other information such as employee department may need to be legitimately accessed by a large number of users. Organizing the data warehouse into subject matter-specific databases is similar to user access in that this control should generally apply. Extra attention could be devoted to reviewing access to tables with sensitive data, but this control is not sufficient without strong preventive controls at the column and row level.
D. Logging user access is important, but it is only a detective control that will not provide adequate protection to sensitive information.

A4-256 The responsibility for authorizing access to a business application system belongs to the:

A. data owner.
B. security administrator.
C. IT security manager.
D. requestor's immediate supervisor.

A is the correct answer.

Justification:

A. **When a business application is developed, a good practice is to assign an information or data owner to the application. The information owner should be responsible for authorizing access to the application itself or to back-end databases for queries.**
B. The security administrator normally does not have responsibility for authorizing access to business applications.
C. The IT security manager normally does not have responsibility for authorizing access to business applications.
D. The requestor's immediate supervisor may share the responsibility for approving user access to a business application system; however, the final responsibility should go to the information owner.

A4-257 What would be the **MOST** effective control for enforcing accountability among database users accessing sensitive information?

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

A is the correct answer.

Justification:

A. **Accountability means knowing what is being done by whom. The best way to enforce the principle is to implement a log management process that would create and store logs with pertinent information such as user name, type of transaction and hour.**
B. Implementing a two-factor authentication would prevent unauthorized access to the database but would not record the activity of the user when using the database.
C. Using table views would restrict users from seeing data that they should not be able to see but would not record what users did with data they were allowed to see.
D. Separating database and application servers may help in better administration or even in implementing access controls but does not address the accountability issues.

A4-258 While auditing an ecommerce architecture, an IS auditor notes that customer master data are stored on the web server for six months after the transaction date and then purged due to inactivity. Which of the following would be the **PRIMARY** concern for the IS auditor?

A. Availability of customer data
B. Integrity of customer data
C. Confidentiality of customer data
D. System storage performance

C is the correct answer.

Justification:

A. Availability of customer data may be affected during an Internet connection outage, but this is of a lower concern than confidentiality.
B. Integrity of customer data is affected only if security controls are weak enough to permit unauthorized modifications to the data, and it may be tracked by logging of changes. Confidentiality of data is a larger concern.
C. **Due to its exposure to the Internet, storing customer data for six months raises concerns regarding confidentiality of customer data.**
D. System storage performance may be a concern due to the volume of data. However, the bigger issue is that the information is protected.

Page intentionally left blank