Question 501
Which of the following systems or tools can recognize that a credit card transaction is more likely to have resulted from a stolen credit card than from the holder of the credit card?
A. Intrusion detection systems
B. Data mining techniques
C. Firewalls
D. Packet filtering routers
Correct Answer: B
Explanation: Data mining techniques can analyze patterns and detect anomalies, such as unusual credit card transactions, helping identify possible fraud.

Question 502
Which of the following would BEST help an IS auditor determine whether there is a segregation of duties issue in a critical IT system?
A. Reviewing user access rights
B. Analyzing job roles and responsibilities
C. Examining the IT organization chart
D. Performing a walkthrough of the business processes
Correct Answer: A
Explanation: Reviewing user access rights helps determine whether individuals have conflicting access to critical systems, which can point to segregation of duties issues.

Question 503
During the development of an application, the quality assurance testing and user acceptance testing were combined. The MAJOR concern for an IS auditor reviewing the project is that there will be:
A. Increased maintenance
B. Improper documentation of testing
C. Inadequate functional testing
D. Delays in problem resolution
Correct Answer: C
Explanation:
The major risk of combining quality assurance testing and user acceptance testing is that functional testing may be inadequate. Choices A, B, and D are not as critical.

Question 504
The GREATEST advantage of rapid application development (RAD) over the traditional system development life cycle (SDLC) is that it:
A. Facilitates user involvement
B. Allows early testing of technical features
C. Facilitates conversion to the new system
D. Shortens the development time frame
Correct Answer: D
Explanation:
The greatest advantage of RAD is the shorter development time frame. Choices A and B are also true but apply to traditional SDLC. Choice C is not necessarily always true.

Question 505
An IS auditor reviewing a proposed application software acquisition should ensure that the:
A. Operating system (OS) being used is compatible with the existing hardware platform
B. Planned OS updates have been scheduled to minimize negative impacts on company needs
C. OS has the latest versions and updates
D. Products are compatible with the current or planned OS

Correct Answer: D
Explanation:
Choices A, B, and C are incorrect because they do not pertain to the area being audited. The auditor should ensure that the products to be purchased are compatible with the current or planned OS.

Question 506
The GREATEST benefit in implementing an expert system is the:
A. Capturing of the knowledge and experience of individuals in an organization
B. Sharing of knowledge in a central repository
C. Enhancement of personnel productivity and performance
D. Reduction of employee turnover in key departments
Correct Answer: A
Explanation:
The basis for an expert system is the capture and recording of knowledge and experience. Enhancing productivity is a benefit, but not as critical as knowledge capture.

Question 507
By evaluating application development projects against the capability maturity model (CMM), an IS auditor should be able to verify that:
A. Reliable products are guaranteed
B. Programmers' efficiency is improved
C. Security requirements are designed
D. Predictable software processes are followed
Correct Answer: D
Explanation:
Evaluating against CMM helps determine whether stable, predictable software processes are followed. Mature processes do not guarantee reliability.

Question 508
The waterfall life cycle model of software development is most appropriately used when:
A. Requirements are well understood and are expected to remain stable, as is the business environment in which the system will operate
B. Requirements are well understood and the project is subject to time pressures
C. The project intends to apply an object-oriented design and programming approach
D. The project will involve the use of new technology
Correct Answer: A
Explanation:
The waterfall model is best suited to stable conditions. Iterative development is better for uncertain environments.

Question 509
Which of the following is MOST critical when creating data for testing the logic in a new or modified application system?
A. A sufficient quantity of data for each test case
B. Data representing conditions that are expected in actual processing
C. Completing the test on schedule
D. A random sample of actual data
Correct Answer: B
Explanation:
Selecting the right data is key; it should be representative of actual processing. Quality is more important than quantity.

Question 510
During the review of a web-based software development project, an IS auditor realizes that coding standards are not enforced and code reviews are rarely carried out. This will MOST likely increase the likelihood of a successful:
A. Buffer overflow
B. Brute force attack
C. Distributed denial-of-service attack
D. War dialing attack
Correct Answer: A
Explanation:
Poorly written code is often exploited through buffer overflow techniques. Other options involve different attack vectors.

Question 511
Which testing approach is MOST appropriate to ensure that internal application interface errors are identified as soon as possible?
A. Bottom up
B. Sociability testing
C. Top-down
D. System test
Correct Answer: C
Explanation:
The top-down approach ensures early detection of interface errors by testing major functions first.

Question 512
During the requirements definition phase of a software development project, the aspects of software testing that should be addressed are developing:
A. Test data covering critical applications
B. Detailed test plans
C. Quality assurance test specifications
D. User acceptance testing specifications
Correct Answer: D
Explanation:
User acceptance test specifications should be developed during the requirements definition phase to ensure the software meets business objectives.

Question 513
Which of the following is an advantage of the top-down approach to software testing?
A. Interface errors are identified early
B. Testing can be started before all programs are complete
C. It is more effective than other testing approaches
D. Errors in critical modules are detected sooner
Correct Answer: A
Explanation:
The top-down approach allows for early testing of major functions, thus detecting interface errors sooner.

Question 514
During the system testing phase of an application development project, the IS auditor should review the:
A. Conceptual design specifications
B. Vendor contract
C. Error reports
D. Program change requests
Correct Answer: C

Explanation:
The IS auditor should review error reports for accuracy in identifying erroneous data and resolution procedures.

Question 515

Which of the following would be the MOST cost-effective recommendation for reducing the number of defects encountered during software development projects?
A. Increase the time allocated for system testing
B. Implement formal software inspections
C. Increase the development staff
D. Require the sign-off of all project deliverables
Correct Answer: B
Explanation:
Formal software inspections are proven techniques to identify defects early in the development life cycle, reducing correction costs.

Question 516

Which of the following is a prevalent risk in the development of end-user computing (EUC) applications?
A. Applications may not be subject to testing and IT general controls
B. Increased development and maintenance costs
C. Increased application development time
D. Decision-making may be impaired due to diminished responsiveness to requests for information
Correct Answer: A
Explanation:
EUC applications may lack appropriate standards, controls, and quality assurance procedures, posing a significant risk.

Question 517

Normally, it would be essential to involve which of the following stakeholders in the initiation stage of a project?
A. System owners
B. System users
C. System designers
D. System builders
Correct Answer: A
Explanation:
System owners are responsible for initiating and funding projects, making their involvement crucial from the start.

Question 518

The MAJOR advantage of a component-based development approach is the:
A. Ability to manage an unrestricted variety of data types
B. Provision for modeling complex relationships
C. Capacity to meet the demands of a changing environment
D. Support of multiple development environments
Correct Answer: D
Explanation:
Component-based development allows interaction between different languages and environments, increasing development speed.

Question 519

The specific advantage of white box testing is that it:

A. Verifies a program can operate successfully with other parts of the system
B. Ensures a program's functional operating effectiveness without regard to the internal program structure
C. Determines procedural accuracy or conditions of a program's specific logic paths
D. Examines a program's functionality by executing it in a tightly controlled or virtual environment with restricted access to the host system
Correct Answer: C
Explanation:
White box testing focuses on assessing the effectiveness of program logic and specific logic paths.

Question 520
Following best practices, formal plans for implementation of new information systems are developed during the:
A. Development phase
B. Design phase
C. Testing phase
D. Deployment phase
Correct Answer: B
Explanation:
Implementation planning should start during the design phase and be revised as development progresses.

Question 521
An IS auditor is reviewing a project that is using an Agile software development approach. Which of the following should the IS auditor expect to find?
A. Use of a process-based maturity model such as the capability maturity model (CMM)
B. Regular monitoring of task-level progress against schedule
C. Extensive use of software development tools to maximize team productivity
D. Post-iteration reviews that identify lessons learned for future use in the project
Correct Answer: D
Explanation:
A key tenet of the Agile approach to software project management is team learning and the use of that learning to refine project management and software development processes as the project progresses. At the end of each iteration, the team considers and documents what worked well and what could have been improved, identifying improvements to implement in subsequent iterations. CMM and Agile operate at opposite ends of the spectrum, as CMM emphasizes predefined formal processes while Agile focuses on adapting processes based on project and team needs.

Question 522
An IS auditor finds that user acceptance testing of a new system is being repeatedly interrupted as defect fixes are implemented by developers. Which of the following would be the BEST recommendation for an IS auditor to make?
A. Consider feasibility of a separate user acceptance environment
B. Schedule user testing to occur at a given time each day
C. Implement a source code version control tool
D. Only retest high priority defects
Correct Answer: A
Explanation:
A separate testing environment is necessary for testing to be efficient and effective and to ensure the integrity of production code. This allows defects to be fixed in the development environment without interrupting testing, and also facilitates regression testing when defects are resolved.

Question 523
Which of the following types of testing would determine whether a new or modified system can operate in its target environment without adversely impacting other existing systems?
A. Parallel testing
B. Pilot testing
C. Interface/integration testing
D. Sociability testing
Correct Answer: D
Explanation:
Sociability testing is designed to confirm that a new or modified system can operate in its target environment without adversely affecting existing systems. It encompasses the overall interaction between systems, while the other testing types focus on different aspects of system performance and integration.

Question 524
At the end of the testing phase of software development, an IS auditor observes that an intermittent software error has not been corrected. No action has been taken to resolve the error. The IS auditor should:
A. Report the error as a finding and leave further exploration to the auditee's discretion.
B. Attempt to resolve the error.
C. Recommend that problem resolution be escalated.
D. Ignore the error, as it is not possible to get objective evidence for the software error.
Correct Answer: C
Explanation:
In this situation, it is appropriate for the auditor to escalate the issue to ensure it is addressed. Reporting it as a minor finding or ignoring it would be inadequate since the auditor has a responsibility to ensure that issues are brought to light and resolved appropriately.

Question 525
Which of the following is an implementation risk within the process of decision support systems?
A. Management control
B. Semistructured dimensions
C. Inability to specify purpose and usage patterns
D. Changes in decision processes
Correct Answer: C
Explanation:
The inability to specify purpose and usage patterns poses a significant risk during the implementation of decision support systems (DSS). The other options describe characteristics or challenges associated with DSS but are not direct implementation risks.

Question 526
An organization is implementing a new system to replace a legacy system. Which of the following conversion practices creates the GREATEST risk?
A. Pilot
B. Parallel
C. Direct cutover
D. Phased
Correct Answer: C
Explanation:
Direct cutover entails switching to the new system immediately, often without the option to revert to the old system if problems arise. This method carries the highest risk compared to other methods, which allow for gradual transitions and provide opportunities for rollback.

Question 527
Which of the following system and data conversion strategies provides the GREATEST redundancy?
A. Direct cutover
B. Pilot study
C. Phased approach
D. Parallel run
Correct Answer: D
Explanation:
Parallel runs allow both the old and new systems to operate concurrently, providing the greatest redundancy and safety, albeit at higher costs. The other methods do not offer the same level of immediate fallback options.

Question 528
Which of the following would impair the independence of a quality assurance team?
A. Ensuring compliance with development methods
B. Checking the testing assumptions
C. Correcting coding errors during the testing process
D. Checking the code to ensure proper documentation
Correct Answer: C
Explanation:
If the quality assurance team is involved in correcting coding errors, it compromises their independence and violates the segregation of duties principle. The other choices are valid QA functions.

Question 529
From a risk management point of view, the BEST approach when implementing a large and complex IT infrastructure is:
A. A big bang deployment after proof of concept.
B. Prototyping and a one-phase deployment.
C. A deployment plan based on sequenced phases.
D. To simulate the new infrastructure before deployment.
Correct Answer: C
Explanation:
Using a phased approach to implement a large and complex IT infrastructure allows for greater assurance of quality results and minimizes risks. Other methods are riskier due to their sudden implementation nature.

Question 530
An organization is migrating from a legacy system to an enterprise resource planning (ERP) system. While reviewing the data migration activity, the MOST important concern for the IS auditor is to determine that there is a:
A. Correlation of semantic characteristics of the data migrated between the two systems.
B. Correlation of arithmetic characteristics of the data migrated between the two systems.
C. Correlation of functional characteristics of the processes between the two systems.
D. Relative efficiency of the processes between the two systems.
Correct Answer: A
Explanation:
The most critical concern during data migration is ensuring that the semantic meaning of the data is preserved across systems, especially since different systems may represent data differently. Arithmetic and functional characteristics are less significant in this context.

Question 531
The reason a certification and accreditation process is performed on critical systems is to ensure that:
A. Security compliance has been technically evaluated.

B. Data have been encrypted and are ready to be stored.
C. The systems have been tested to run on different platforms.
D. The systems have followed the phases of a waterfall model.
Correct Answer: A
Explanation:
The certification and accreditation process ensures that the security compliance of critical systems has been evaluated. It is not specifically about data encryption or platform compatibility, nor is it tied to a particular software development methodology.

Question 532
An IS auditor who has discovered unauthorized transactions during a review of EDI transactions is likely to recommend improving the:
A. EDI trading partner agreements.
B. Physical controls for terminals.
C. Authentication techniques for sending and receiving messages.
D. Program change control procedures.
Correct Answer: C
Explanation:
Authentication techniques for sending and receiving messages play a key role in minimizing exposure to unauthorized transactions. The EDI trading partner agreements would minimize exposure to legal issues.

Question 533
An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:
A. Check to ensure that the type of transaction is valid for the card type.
B. Verify the format of the number entered then locate it on the database.
C. Ensure that the transaction entered is within the cardholder's credit limit.
D. Confirm that the card is not shown as lost or stolen on the master file.
Correct Answer: B
Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed.

Question 534
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?
A. Key verification.
B. One-for-one checking.
C. Manual recalculations.
D. Functional acknowledgements.
Correct Answer: D
Explanation:
Functional acknowledgements act as an audit trail for EDI transactions and are one of the main controls used in data mapping, ensuring the efficient integration of data in the receiving company.

Question 535
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:
A. Pre-BPR process flowcharts.
B. Post-BPR process flowcharts.
C. BPR project plans.
D. Continuous improvement and monitoring plans.
Correct Answer: B

Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Reviewing post-BPR process flowcharts provides the necessary insight into the current state of controls.

Question 536
A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:
A. Payroll reports should be compared to input forms.
B. Gross payroll should be recalculated manually.
C. Checks (cheques) should be compared to input forms.
D. Checks (cheques) should be reconciled with output reports.
Correct Answer: A
Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports.

Question 537
Which of the following represents the GREATEST potential risk in an EDI environment?
A. Transaction authorization.
B. Loss or duplication of EDI transmissions.
C. Transmission delay.
D. Deletion or manipulation of transactions prior to or after establishment of application controls.
Correct Answer: A
Explanation:
Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk.

Question 538
Which of the following is the MOST critical and contributes the greatest 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.
Correct Answer: A
Explanation:
Accuracy of source data is a prerequisite for the quality of the data in a data warehouse.

Question 539
When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?
A. Use of a cryptographic hashing algorithm.
B. Enciphering the message digest.
C. Deciphering the message digest.
D. A sequence number and time stamp.
Correct Answer: D
Explanation:
A sequence number and/or time stamp built into the message can be checked by the recipient to ensure that the message was not intercepted and replayed, thus preventing duplication.

Question 540

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:
A. Not be concerned since there may be other compensating controls to mitigate the risks.
B. Ensure that overrides are automatically logged and subject to review.
C. Verify whether all such overrides are referred to senior management for approval.
D. Recommend that overrides not be permitted.
Correct Answer: B
Explanation:
If input procedures allow overrides of data validation and editing, automatic logging should occur, and a management individual who did not initiate the override should review this log.

Question 541
When using an integrated test facility (ITF), an IS auditor should ensure that:
A. Production data are used for testing.
B. Test data are isolated from production data.
C. A test data generator is used.
D. Master files are updated with the test data.
Correct Answer: B
Explanation:
An integrated test facility creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data, while ensuring that test data is isolated from production data.

Question 542
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.
Correct Answer: A
Explanation:
Choice A would prevent or detect the use of an unauthorized interest rate. It ensures that management is involved in the approval process before the change is processed.

Question 543
An IS auditor recommends that an initial validation control be programmed into a credit card transaction capture application. The initial validation process would MOST likely:
A. Check to ensure that the type of transaction is valid for the card type.
B. Verify the format of the number entered then locate it on the database.
C. Ensure that the transaction entered is within the cardholder's credit limit.
D. Confirm that the card is not shown as lost or stolen on the master file.
Correct Answer: B
Explanation:
The initial validation should confirm whether the card is valid. This validity is established through the card number and PIN entered by the user. Based on this initial validation, all other validations will proceed.

Question 544
A company has recently upgraded its purchase system to incorporate EDI transmissions. Which of the following controls should be implemented in the EDI interface to provide for efficient data mapping?

A. Key verification.
B. One-for-one checking.
C. Manual recalculations.
D. Functional acknowledgements.
Correct Answer: D
Explanation:
Functional acknowledgements act as an audit trail for EDI transactions and are one of the main controls used in data mapping, ensuring the efficient integration of data in the receiving company.

Question 545
Once an organization has finished the business process reengineering (BPR) of all its critical operations, an IS auditor would MOST likely focus on a review of:
A. Pre-BPR process flowcharts.
B. Post-BPR process flowcharts.
C. BPR project plans.
D. Continuous improvement and monitoring plans.
Correct Answer: B
Explanation:
An IS auditor's task is to identify and ensure that key controls have been incorporated into the reengineered process. Reviewing post-BPR process flowcharts provides the necessary insight into the current state of controls.

Question 546
A company uses a bank to process its weekly payroll. Time sheets and payroll adjustment forms (e.g., hourly rate changes, terminations) are completed and delivered to the bank, which prepares checks (cheques) and reports for distribution. To BEST ensure payroll data accuracy:
A. Payroll reports should be compared to input forms.
B. Gross payroll should be recalculated manually.
C. Checks (cheques) should be compared to input forms.
D. Checks (cheques) should be reconciled with output reports.
Correct Answer: A
Explanation:
The best way to confirm data accuracy, when input is provided by the company and output is generated by the bank, is to verify the data input (input forms) with the results of the payroll reports.

Question 547
Which of the following represents the GREATEST potential risk in an EDI environment?
A. Transaction authorization.
B. Loss or duplication of EDI transmissions.
C. Transmission delay.
D. Deletion or manipulation of transactions prior to or after establishment of application controls.
Correct Answer: A
Explanation:
Since the interaction between parties is electronic, there is no inherent authentication occurring; therefore, transaction authorization is the greatest risk.

Question 548
Which of the following is the MOST critical and contributes the greatest 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.

Correct Answer: A

Explanation:

Accuracy of source data is a prerequisite for the quality of the data in a data warehouse.

Question 549

When transmitting a payment instruction, which of the following will help verify that the instruction was not duplicated?

A. Use of a cryptographic hashing algorithm.

B. Enciphering the message digest.

C. Deciphering the message digest.

D. A sequence number and time stamp.

Correct Answer: D

Explanation:

A sequence number and/or time stamp built into the message can be checked by the recipient to ensure that the message was not intercepted and replayed, thus preventing duplication.

Question 550

When reviewing input controls, an IS auditor observes that, in accordance with corporate policy, procedures allow supervisory override of data validation edits. The IS auditor should:

A. Not be concerned since there may be other compensating controls to mitigate the risks.

B. Ensure that overrides are automatically logged and subject to review.

C. Verify whether all such overrides are referred to senior management for approval.

D. Recommend that overrides not be permitted.

Correct Answer: B

Explanation:

If input procedures allow overrides of data validation and editing, automatic logging should occur, and a management individual who did not initiate the override should review this log.

Question 551

When using an integrated test facility (ITF), an IS auditor should ensure that:

A. Production data are used for testing.

B. Test data are isolated from production data.

C. A test data generator is used.

D. Master files are updated with the test data.

Correct Answer: B

Explanation:

An integrated test facility creates a fictitious file in the database, allowing for test transactions to be processed simultaneously with live data, while ensuring that test data is isolated from production data.

Question 552

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.

Correct Answer: A

Explanation:

Choice A would prevent or detect the use of an unauthorized interest rate. It ensures that management is involved in the approval process before the change is processed.

Question 553

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

A. secure communications.
B. improved performance.
C. efficient interfacing.
D. enhanced documentation.

Correct Answer: C

Explanation:

Web services facilitate the exchange of information between two systems, regardless of the operating system or programming language used. Communication is not necessarily securer or faster, and there is no documentation benefit in using web services.

Question 554

An IS auditor reviewing an accounts payable system discovers that audit logs are not being reviewed. When this issue is raised with management the response is that additional controls are not necessary because effective system access controls are in place. The BEST response the auditor can make is to:

A. review the integrity of system access controls.
B. accept management's statement that effective access controls are in place.
C. stress the importance of having a system control framework in place.
D. review the background checks of the accounts payable staff.

Correct Answer: C

Explanation:

Experience has demonstrated that reliance purely on preventative controls is dangerous. Preventative controls may not prove to be as strong as anticipated or their effectiveness can deteriorate over time. Evaluating the cost of controls versus the quantum of risk is a valid management concern. However, in a high-risk system, a comprehensive control framework is needed, intelligent design should permit additional detective and corrective controls to be established that don't have high ongoing costs, e.g., automated interrogation of logs to highlight suspicious individual transactions or data patterns. Effective access controls are, in themselves, a positive but, for reasons outlined above, may not sufficiently compensate for other control weaknesses. In this situation, the IS auditor needs to be proactive. The IS auditor has a fundamental obligation to point out control weaknesses that give rise to unacceptable risks to the organization and work with management to have these corrected. Reviewing background checks on accounts payable staff does not provide evidence that fraud will not occur.

Question 555

When evaluating the controls of an EDI application, an IS auditor should PRIMARILY be concerned with the risk of:

A. excessive transaction turnaround time.
B. application interface failure.
C. improper transaction authorization.
D. nonvalidated batch totals.

Correct Answer: C

Explanation:

Foremost among the risks associated with electronic data interchange (EDI) is improper transaction authorization. Since the interaction with the parties is electronic, there is no inherent authentication. The other choices, although risks, are not as significant.

Question 556

When reviewing an organization's approved software product list, which of the following is the MOST important thing to verify?

A. The risks associated with the use of the products are periodically assessed.
B. The latest version of software is listed for each product.
C. Due to licensing issues, the list does not contain open source software.
D. After hours support is offered.
Correct Answer: A
Explanation:
Since the business conditions surrounding vendors may change, it is important for an organization to conduct periodic risk assessments of the vendor software list. This might be best incorporated into the IT risk management process. Choices B, C, and D are possible considerations but would not be the most important.

Question 557
An existing system is being extensively enhanced by extracting and reusing design and program components. This is an example of:
A. reverse engineering.
B. prototyping.
C. software reuse.
D. reengineering.
Correct Answer: D
Explanation:
Old (legacy) systems that have been corrected, adapted, and enhanced extensively require reengineering to remain maintainable. Reengineering is a rebuilding activity to incorporate new technologies into existing systems. Using program language statements, reverse engineering involves reversing a program's machine code into the source code in which it was written to identify malicious content in a program, such as a virus, or to adapt a program written for use with one processor for use with a differently designed processor. Prototyping is the development of a system through controlled trial and error. Software reuse is the process of planning, analyzing, and using previously developed software components. The reusable components are integrated into the current software product systematically.

Question 558
A number of system failures are occurring when corrections to previously detected errors are resubmitted for acceptance testing. This would indicate that the maintenance team is probably not performing adequately which of the following types of testing?
A. Unit testing
B. Integration testing
C. Design walkthroughs
D. Configuration management
Correct Answer: B
Explanation:
A common system maintenance problem is that errors are often corrected quickly (especially when deadlines are tight). Units are tested by the programmer and then transferred to the acceptance test area; this often results in system problems that should have been detected during integration or system testing. Integration testing aims at ensuring that the major components of the system interface correctly.

Question 559
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.
Correct Answer: A

Explanation:
The manual log will most likely contain information on authorized changes to a program. Deliberate, unauthorized changes will not be documented by the responsible party. An automated log, found usually in library management products, and not a changelog would most likely contain date information for the source and executable modules.

Question 560
After discovering a security vulnerability in a third-party application that interfaces with several external systems, a patch is applied to a significant number of modules. Which of the following tests should an IS auditor recommend?
A. Stress
B. Black box
C. Interface
D. System
Correct Answer: D
Explanation:
Given the extensiveness of the patch and its interfaces to external systems, system testing is most appropriate. Interface testing is not enough, and stress or black box testing are inadequate in these circumstances.

Question 561
When performing an audit of a client relationship management (CRM) system migration project, which of the following should be of GREATEST concern to an IS auditor?
A. The technical migration is planned for a Friday preceding a long weekend, and the time window is too short for completing all tasks.
B. Employees pilot-testing the system are concerned that the data representation in the new system is completely different from the old system.
C. A single implementation is planned, immediately decommissioning the legacy system.
D. Five weeks prior to the target date, there are still numerous defects in the printing functionality of the new system's software.
Correct Answer: C
Explanation:
Major system migrations should include a phase of parallel operation or a phased cut-over to reduce implementation risks. Decommissioning or disposing of the old hardware would complicate any fallback strategy should the new system not operate correctly. A weekend can be used as a time buffer so that the new system will have a better chance of being up and running after the weekend. A different data representation does not mean different data presentation at the front end. Even when this is the case, this issue can be solved by adequate training and user support. The printing functionality is commonly one of the last functions to be tested in a new system because it is usually the last step performed in any business event. Thus, meaningful testing and the respective error fixing are only possible after all other parts of the software have been successfully tested.

Question 562
Which of the following reports should an IS auditor use to check compliance with a service level agreement's (SLA) requirement for uptime?
A. Utilization reports
B. Hardware error reports
C. System logs
D. Availability reports
Correct Answer: D
Explanation:
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. Utilization reports document the use of computer equipment and can be used by management to predict how/where/when resources are required. Hardware error reports provide information to aid in detecting hardware failures and initiating corrective action. System logs are a recording of the system's activities.

Question 563

A benefit of quality of service (QoS) is that the:
A. entire network's availability and performance will be significantly improved.
B. telecom carrier will provide the company with accurate service-level compliance reports.
C. participating applications will have guaranteed service levels.
D. communications link will be supported by security controls to perform secure online transactions.

Correct Answer: C

Explanation:
The main function of QoS is to optimize network performance by assigning priority to business applications and end users through the allocation of dedicated parts of the bandwidth to specific traffic. Choice A is not true because the communication itself will not be improved. While the speed of data exchange for specific applications could be faster, availability will not be improved. The QoS tools that many carriers are using do not provide reports of service levels; however, there are other tools that will generate service-level reports. Even when QoS is integrated with firewalls, VPNs, encryption tools, and others, the tool itself is not intended to provide security controls.

Question 564

An organization has outsourced its help desk. Which of the following indicators would be the best to include in the SLA?
A. Overall number of users supported
B. Percentage of incidents solved in the first call
C. Number of incidents reported to the help desk
D. Number of agents answering the phones

Correct Answer: B

Explanation:
Since it is about service level (performance) indicators, the percentage of incidents solved on the first call is the only option that is relevant. Choices A, C, and D are not quality measures of the help desk service.

Question 565

The PRIMARY objective of service-level management (SLM) is to:
A. define, agree, 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.

Correct Answer: A

Explanation:
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. This 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. SLM cannot ensure that costs for all services will be kept at a low or minimum level since costs associated with a service will directly reflect the customer's requirements. Monitoring and reporting legal noncompliance is not a part of SLM.

Question 566

Which of the following should be of PRIMARY concern to an IS auditor reviewing the management of external IT service providers?
A. Minimizing costs for the services provided

B. Prohibiting the provider from subcontracting services
C. Evaluating the process for transferring knowledge to the IT department
D. Determining if the services were provided as contracted

Correct Answer: D

Explanation:

From an IS auditor's perspective, the primary objective of auditing the management of service providers should be to determine if the services that were requested were provided in a way that is acceptable, seamless, and in line with contractual agreements. Minimizing costs, if applicable and achievable (depending on the customer's need), is traditionally not part of an IS auditor's job. This would normally be done by a line management function within the IT department. Furthermore, during an audit, it is too late to minimize the costs for existing provider arrangements. Subcontracting providers could be a concern, but it would not be the primary concern. Transferring knowledge to the internal IT department might be desirable under certain circumstances, but should not be the primary concern of an IS auditor when auditing IT service providers and the management thereof.

Question 567

IT best practices for the availability and continuity of IT services should:
A. minimize costs associated with disaster-resilient components.
B. provide for sufficient capacity to meet the agreed-upon demands of the business.
C. provide reasonable assurance that agreed-upon obligations to customers can be met.
D. produce timely performance metric reports.

Correct Answer: C

Explanation:

It is important that negotiated and agreed commitments (i.e., service level agreements [SLAs]) can be fulfilled all the time. If this were not achievable, IT should not have agreed to these requirements, as entering into such a commitment would be misleading to the business. 'All the time' in this context directly relates to the 'agreed obligations' and does not imply that a service has to be available 100 percent of the time. Costs are a result of availability and service continuity management and may only be partially controllable. These costs directly reflect the agreed-upon obligations. Capacity management is necessary but not sufficient for availability. Despite the possibility that a lack of capacity may result in an availability issue, providing the necessary capacity for seamless operations of services would be done within capacity management, and not within availability management. Generating reports might be a task of availability and service continuity management, but that is true for many other areas of interest as well (e.g., incident, problem, capacity, and change management).

Question 568

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 (SLA) for the two departments

Correct Answer: C

Explanation:

An IS auditor should first confirm and understand the current practice before making any recommendations. The agreement can be documented after it has been established that there is an agreement in place. The fact that there is not a written agreement does not justify postponing the audit, and reporting to senior management is not necessary at this stage of the audit. Drafting a service level agreement (SLA) is not the IS auditor's responsibility.

Question 569

Which of the following procedures would MOST effectively detect the loading of illegal software packages onto a network?
A. The use of diskless workstations
B. Periodic checking of hard drives
C. The use of current antivirus software
D. Policies that result in instant dismissal if violated
Correct Answer: B
Explanation:
The periodic checking of hard drives would be the most effective method of identifying illegal software packages loaded onto the network. Antivirus software will not necessarily identify illegal software unless the software contains a virus. Diskless workstations act as a preventive control and are not effective since users could still download software from other than diskless workstations. Policies lay out the rules about loading the software, but will not detect the actual occurrence.

Question 570
To determine which users can gain access to the privileged supervisory state, which of the following should an IS auditor review?
A. System access log files
B. Enabled access control software parameters
C. Logs of access control violations
D. System configuration files for control options used
Correct Answer: D
Explanation:
A review of system configuration files for control options used would show which users have access to the privileged supervisory state. Both system access log files and logs of access violations are detective in nature. Access control software is run under the operating system.

Question 571
Which of the following would an IS auditor consider to be the MOST helpful when evaluating the effectiveness and adequacy of a computer preventive maintenance program?
A. A system downtime log
B. Vendors' reliability figures
C. Regularly scheduled maintenance log
D. A written preventive maintenance schedule
Correct Answer: A
Explanation:
A system downtime log provides information regarding the effectiveness and adequacy of computer preventive maintenance programs.

Question 572
Which of the following exposures associated with the spooling of sensitive reports for offline printing should an IS auditor consider to be the MOST serious?
A. Sensitive data can be read by operators.
B. Data can be amended without authorization.
C. Unauthorized report copies can be printed.
D. Output can be lost in the event of system failure.
Correct Answer: C
Explanation:
Unless controlled, spooling for offline printing may enable additional copies to be printed. Print files are unlikely to be available for online reading by operators. Data on spool files are no easier to amend without authority than any other file. There is usually a lesser threat of unauthorized access to sensitive reports in the event of a system failure.

Question 573
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.
Correct Answer: B
Explanation:
A retention date will ensure that a file cannot be overwritten before that date has passed. The retention date will not affect the ability to read the file. Backup copies would be expected to have a different retention date and therefore may be retained after the file has been overwritten. The creation date, not the retention date, will differentiate files with the same name.

Question 574
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
Correct Answer: D
Explanation:
Protocol analyzers are network diagnostic tools that monitor and record network information from packets traveling in the link to which the analyzer is attached. Online monitors measure telecommunications transmissions and determine whether transmissions were accurate and complete. Downtime reports track the availability of telecommunication lines and circuits. 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.

Question 575
Which of the following will help detect changes made by an intruder to the system log of a server?
A. Mirroring the system log on another server
B. Simultaneously duplicating the system log on a write-once disk
C. Write-protecting the directory containing the system log
D. Storing the backup of the system log offsite
Correct Answer: B
Explanation:
A write-once CD cannot be overwritten. Therefore, the system log duplicated on the disk could be compared to the original log to detect differences, which could be the result of changes made by an intruder. Write-protecting the system log does not prevent deletion or modification, since the superuser can override the write protection. Backup and mirroring may overwrite earlier files and may not be current.

Question 576
IT operations for a large organization have been outsourced. An IS auditor reviewing the outsourced operation should be MOST concerned about which of the following findings?
A. The outsourcing contract does not cover disaster recovery for the outsourced IT operations.
B. The service provider does not have incident handling procedures.
C. Recently a corrupted database could not be recovered because of library management problems.
D. Incident logs are not being reviewed.
Correct Answer: A
Explanation:
The lack of a disaster recovery provision presents a major business risk. Incorporating such a provision

into the contract will provide the outsourcing organization leverage over the service provider. Choices B, C, and D are problems that should be addressed by the service provider but are not as important as contract requirements for disaster recovery.

Question 577

Which of the following BEST ensures the integrity of a server's operating system?
A. Protecting the server in a secure location
B. Setting a boot password
C. Hardening the server configuration
D. Implementing activity logging

Correct Answer: C

Explanation:

Hardening a system means to configure it in the most secure manner (install the latest security patches, properly define the access authorization for users and administrators, disable insecure options, and uninstall unused services) to prevent nonprivileged users from gaining the right to execute privileged instructions and thus take control of the entire machine, jeopardizing the OS's integrity. Protecting the server in a secure location and setting a boot password are good practices, but do not ensure that a user will not try to exploit logical vulnerabilities and compromise the OS. Activity logging has two weaknesses in this scenario: it is a detective control (not a preventive one), and the attacker who has already gained privileged access can modify logs or disable them.

Question 578

The MOST significant security concern when using flash memory (e.g., USB removable disk) is that the:
A. contents are highly volatile.
B. data cannot be backed up.
C. data can be copied.
D. device may not be compatible with other peripherals.

Correct Answer: C

Explanation:

Unless properly controlled, flash memory provides an avenue for anyone to copy any content with ease. The contents stored in flash memory are not volatile. Backing up flash memory data is not a control concern, as the data are sometimes stored as a backup. Flash memory will be accessed through a PC rather than any other peripheral; therefore, compatibility is not an issue.

Question 579

The database administrator (DBA) suggests that DB 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.

Correct Answer: B

Explanation:

Normalization is a design or optimization process for a relational database that minimizes redundancy; therefore, denormalization would increase redundancy. Redundancy, which is usually considered positive when it is a question of resource availability, is negative in a database environment since it demands additional and otherwise unnecessary data handling efforts. Denormalization is sometimes advisable for functional reasons. It should not cause loss of confidentiality, unauthorized accesses, or application malfunctions.

Question 580

Web and e-mail filtering tools are PRIMARILY valuable to an organization because they:
A. protect the organization from viruses and nonbusiness materials.
B. maximize employee performance.
C. safeguard the organization's image.
D. assist the organization in preventing legal issues.
Correct Answer: A
Explanation:
The main reason for investing in web and e-mail filtering tools is that they significantly reduce risks related to viruses, spam, mail chains, recreational surfing, and recreational e-mail. Choice B could be true in some circumstances (i.e., it would need to be implemented along with an awareness program so that employee performance can be significantly improved). However, in such cases, it would not be as relevant as choice A. Choices C and D are secondary or indirect benefits.

QUESTION 581
The BEST way to minimize the risk of communication failures in an e-commerce environment would be to use:
- Compression software to minimize transmission duration.
- Functional or message acknowledgments.
- A packet-filtering firewall to reroute messages.
- Leased asynchronous transfer mode lines.
Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Leased asynchronous transfer mode lines avoid using public and shared infrastructures that have a greater number of communication failures. Compression software reduces transmission time but is not as effective as leased lines. Functional acknowledgments help if communication lines introduce noise but don't assist if a link is down. A packet-filtering firewall does not reroute messages.

QUESTION 582
An IS auditor reviewing an organization's data file control procedures finds that transactions are applied to the most current files, while restart procedures use earlier versions. The IS auditor should recommend the implementation of:
- Source documentation retention.
- Data file security.
- Version usage control.
- One-for-one checking.
Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Proper version usage is essential to ensure that the correct database version is used for transactions and restarts. Source documentation retention helps with verification but does not ensure the use of the correct file. Data file security prevents unauthorized access but does not address versioning. One-for-one checking ensures that all documents are processed but does not ensure the correct version is used.

QUESTION 583
Which of the following BEST limits the impact of server failures in a distributed environment?
- Redundant pathways
- Clustering
- Dial backup lines
- Standby power
Correct Answer: B

Explanation:
Clustering allows multiple servers to operate as a unit, ensuring that when one fails, another can take over. Redundant pathways and dial backup lines are designed for communication failures, not server failures. Standby power provides an alternative power source but does not address server failures.

QUESTION 584
When reviewing a hardware maintenance program, an IS auditor should assess whether:
- The schedule of all unplanned maintenance is maintained.
- It is in line with historical trends.
- It has been approved by the IS steering committee.
- The program is validated against vendor specifications.

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
The maintenance program should be validated against vendor specifications to ensure it meets the hardware's operational needs. Unplanned maintenance cannot be scheduled, and maintenance programs do not require approval by the steering committee or alignment with historical trends.

QUESTION 585
An IS auditor observes a weakness in the tape management system at a data center in that some parameters are set to bypass or ignore tape header records. Which of the following is the MOST effective compensating control for this weakness?
- Staging and job setup
- Supervisory review of logs
- Regular back-up of tapes
- Offsite storage of tapes

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Effective staging and job setup can act as a compensating control for the weakness found in tape management. Supervisory review is a detective control, while regular backups and offsite storage are corrective controls that do not directly address the bypass of tape header records.

QUESTION 586
To verify that the correct version of a data file was used for a production run, an IS auditor should review:
- Operator problem reports.
- Operator work schedules.
- System logs.
- Output distribution reports.

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
System logs provide automated reports identifying activities performed on the computer, allowing the auditor to verify the correct file version was used. Operator problem reports and work schedules do not assist in this verification, and output distribution reports focus on report generation rather than file version usage.

QUESTION 587
Which of the following is the BEST type of program for an organization to implement to aggregate, correlate, and store different log and event files, and then produce weekly and monthly reports for IS auditors?

- A security information event management (SIEM) product
- An open-source correlation engine
- A log management tool
- An extract, transform, load (ETL) system

Correct Answer: C
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
A log management tool is specifically designed for aggregating and storing log events from various sources and producing reports, making it the best choice. A SIEM product has similar features but is not primarily focused on long-term storage and reporting of logs. An open-source correlation engine is a part of a SIEM, while an ETL system is unrelated to log management.

QUESTION 588
Doing which of the following during peak production hours could result in unexpected downtime?
- Performing data migration or tape backup
- Performing preventive maintenance on electrical systems
- Promoting applications from development to the staging environment
- Replacing a failed power supply in the core router of the data center

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Preventive maintenance activities should ideally be scheduled during non-peak times. Performing such maintenance during peak hours could inadvertently lead to unplanned downtime, whereas the other options generally do not cause downtime.

QUESTION 589
Which of the following would BEST maintain the integrity of a firewall log?
- Granting access to log information only to administrators
- Capturing log events in the operating system layer
- Writing dual logs onto separate storage media
- Sending log information to a dedicated third-party log server

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Establishing a dedicated third-party log server enhances log integrity by reducing the risk of unauthorized modifications. Limited access to log information primarily supports confidentiality rather than integrity. Capturing logs in the operating system layer does not enhance integrity, and dual logs mainly ensure availability rather than integrity.

QUESTION 590
Which of the following will prevent dangling tuples in a database?
- Cyclic integrity
- Domain integrity
- Relational integrity
- Referential integrity

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Referential integrity ensures that all foreign keys in a table have corresponding primary keys in another table, thus preventing dangling tuples. Cyclic integrity is not a recognized term, domain integrity relates to data value ranges, and relational integrity pertains to record-level validation.

QUESTION 591
The objective of concurrency control in a database system is to:
- Restrict updating of the database to authorized users.
- Prevent integrity problems when two processes attempt to update the same data at the same time.
- Prevent inadvertent or unauthorized disclosure of data in the database.
- Ensure the accuracy, completeness, and consistency of data.

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Concurrency controls are designed to prevent data integrity issues when multiple processes try to access the same data simultaneously. The other options relate to access controls and data quality but do not specifically address concurrency.

QUESTION 592
Which of the following controls would provide the GREATEST assurance of database integrity?
- Audit log procedures
- Table link/reference checks
- Query/table access time checks
- Rollback and rollforward database features

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Table link/reference checks detect linking errors and ensure completeness and accuracy of database contents, providing the highest assurance of integrity. Audit logs help trace events but do not ensure database content integrity. Query checks improve performance, and rollback features focus on transaction recovery rather than overall database integrity.

QUESTION 593
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 are not rolled back. Which of the following transaction processing features has been violated?
- Consistency
- Isolation
- Durability
- Atomicity

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Atomicity ensures that transactions are fully processed or not at all. If a transaction is partially executed without rollback, atomicity is violated. Consistency ensures legal database states, isolation keeps transactions invisible to each other during processing, and durability ensures completed transactions persist.

QUESTION 594
During maintenance of a relational database, several values of the foreign key in a transaction table of a relational database have been corrupted. The consequence is that:
- The detail of involved transactions may no longer be associated with master data, causing errors when these transactions are processed.
- There is no way of reconstructing the lost information, except by deleting the dangling tuples and reentering the transactions.
- The database will immediately stop execution and lose more information.

- The database will no longer accept input data.

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Corruption of foreign keys prevents the application from correctly associating master data with transaction data, which can lead to processing errors. The other options incorrectly suggest immediate or severe consequences from foreign key corruption.

QUESTION 595
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?
- Foreign key
- Primary key
- Secondary key
- Public key

Correct Answer: A
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Foreign keys enforce referential integrity, preventing deletions that would result in orphaned records in related tables. Primary keys identify records within a single table, while secondary and public keys do not enforce referential relationships.

QUESTION 596
Which of the following types of controls would MOST likely ensure the reliability of a network in an organization?
- Physical controls
- Management controls
- Operational controls
- Technical controls

Correct Answer: D
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Technical controls, such as firewalls, intrusion detection systems, and encryption, are essential for ensuring the reliability and security of a network. Physical controls focus on protecting hardware, while management and operational controls relate to policies and procedures but do not directly ensure network reliability.

QUESTION 597
An organization wants to ensure that its database transactions are processed accurately and reliably. Which of the following is the MOST appropriate method to achieve this?
- Implementing a high-availability configuration
- Using transaction logging
- Performing regular backups
- Applying encryption techniques

Correct Answer: B
Section: IT SERVICE DELIVERY AND SUPPORT
Explanation:
Transaction logging captures all changes made to the database, enabling accurate recovery and rollback in case of errors, thus ensuring the reliability of transactions. High-availability configurations improve uptime but do not address transaction accuracy. Backups are important but do not ensure transaction reliability in real-time, and encryption protects data confidentiality rather than transaction accuracy.

QUESTION 598

Which of the following BEST describes the purpose of a change management process in IT?

- To minimize the risk of downtime during system upgrades.
- To document all technical specifications for future reference.
- To control and manage changes to IT systems and infrastructure.
- To ensure compliance with regulatory requirements.

Correct Answer: C

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

The primary purpose of change management is to control and manage changes to IT systems and infrastructure to minimize disruption and maintain system integrity. While minimizing downtime and ensuring compliance are important, they are not the main focus of change management.

QUESTION 599

When evaluating the effectiveness of a disaster recovery plan, an IS auditor should FIRST verify that:

- Backup procedures are documented and updated regularly.
- Business impact analyses have been performed.
- Recovery time objectives (RTO) are clearly defined.
- The plan is tested and the results documented.

Correct Answer: D

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

Testing the disaster recovery plan and documenting the results is essential to ensure that it works as intended. While the other options are important, the effectiveness of a plan is primarily demonstrated through testing.

QUESTION 600

An organization is planning to implement a new information system. The MOST important factor to consider during the system's design phase is:

- Integration with existing systems.
- Compliance with regulatory requirements.
- User training and support.
- Data migration strategies.

Correct Answer: A

Section: IT SERVICE DELIVERY AND SUPPORT

Explanation:

Integration with existing systems is crucial to ensure the new system operates effectively within the organization's IT environment. Compliance, training, and data migration are also important but secondary to ensuring seamless integration.