ISACA Journal, vol. 2, 2012, *https://www.isaca.org/Journal/archives/2012/Volume-2/Pages/Testing-Controls-Associated-With-Data-Transfers.aspx*

SELF-ASSESSMENT QUESTIONS

CISA self-assessment questions support the content in this manual and provide an understanding of the type and structure of questions that typically appear on the exam. Often, a question will require the candidate to choose the **MOST** likely or **BEST** answer among the options provided. Please note that these questions are not actual or retired exam items. Please see the section "About This Manual" at the beginning of this manual for more guidance regarding practice questions.

3-1 To assist in testing an essential banking system being acquired, an organization has provided the vendor with sensitive data from its existing production system. An IS auditor's **PRIMARY** concern is that the data should be:

A. sanitized.
B. complete.
C. representative.
D. current.

3-2 Which of the following is the **PRIMARY** purpose for conducting parallel testing?

A. To determine whether the system is cost-effective
B. To enable comprehensive unit and system testing
C. To highlight errors in the program interfaces with files
D. To ensure the new system meets user requirements

3-3 When conducting a review of business process reengineering, an IS auditor found that an important preventive control had been removed.

In this case, the IS auditor should:

A. inform management of the finding and determine whether management is willing to accept the potential material risk of not having that preventive control.
B. determine if a detective control has replaced the preventive control during the process, and if it has not, report the removal of the preventive control.
C. recommend that this and all control procedures that existed before the process was reengineered be included in the new process.
D. develop a continuous audit approach to monitor the effects of the removal of the preventive control.

3-4 Which of the following data validation edits is effective in detecting transposition and transcription errors?

A. Range check
B. Check digit
C. Validity check
D. Duplicate check

3-5 Which of the following weaknesses would be considered the **MOST** serious in enterprise resource planning software used by a financial organization?

A. Access controls have not been reviewed.
B. Limited documentation is available.
C. Two-year-old backup tapes have not been replaced.
D. Database backups are performed once a day.

3-6 When auditing the requirements phase of a software acquisition, an IS auditor should:

A. assess the reasonability of the project timetable.

B. assess the vendor's proposed quality processes.
C. ensure that the best software package is acquired.
D. review the completeness of the specifications.

3-7 An organization decides to purchase a software package instead of developing it. In such a case, the design and development phases of a traditional system development life cycle would be replaced with:

A. selection and configuration phases
B. feasibility and requirements phases
C. implementation and testing phases
D. nothing, as replacement is not required.

3-8 User specifications for a software development project using the traditional (waterfall) system development life cycle methodology have not been met. An IS auditor looking for a cause should look in which of the following areas?

A. Quality assurance
B. Requirements
C. Development
D. User training

3-9 When introducing thin client architecture, which of the following types of risk regarding servers is significantly increased?

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

3-10 Which of the following procedures should be implemented to help ensure the completeness of inbound transactions via electronic data

interchange (EDI)?

A. Segment counts built into the transaction set trailer
B. A log of the number of messages received, periodically verified with the transaction originator
C. An electronic audit trail for accountability and tracking
D. Matching acknowledgment transactions received to the log of EDI messages sent

ANSWERS TO SELF-ASSESSMENT QUESTIONS

3-1 **A. Test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.**

B. Although it is important that the data set be complete, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

C. Although it is important to encompass a representation of the transactional data, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

D. Although it is important that the data set represent current data being processed, the primary concern is that test data should be sanitized to prevent sensitive data from leaking to unauthorized persons.

3-2 A. Parallel testing may show that the old system is more cost-effective than the new system, but this is not the primary reason.

B. Unit and system testing are completed before parallel testing.

C. Program interfaces with files are tested for errors during system testing.

D. The purpose of parallel testing is to ensure that the implementation of a new system will meet user requirements.

3-3 **A. Those in management should be informed immediately to determine whether they are willing to accept the potential material risk of not having that preventive control in place.**

B. The existence of a detective control instead of a preventive control usually increases the risk that a material problem may occur.

C. Often during business process reengineering, many nonvalue-added controls will be eliminated. This is good, unless they increase the business and financial risk.

D. An IS auditor may wish to monitor or recommend that management monitor the new process, but this should be done only after management has been informed and accepts the risk of not having the preventive control in place.

3-4 A. A range check is checking data that match a predetermined range of values.

B. A check digit is a numeric value that is calculated mathematically and is appended to data to ensure that the original data have not been altered (e.g., an incorrect, but valid, value substituted for the original). This control is effective in detecting transposition and transcription errors.

C. An availability check is programmed checking of the data validity in accordance with predetermined criteria.

D. In a duplicate check, new or fresh transactions are matched to those previously entered to ensure that they are not already in the system.

3-5 **A. A lack of review of access controls in a financial organization could have serious consequences given the types of data and assets that could be accessed.**

B. A lack of documentation may not be as serious as not having properly reviewed access controls.

C. It may not even be possible to retrieve data from two-year-old backup tapes.

D. It may be acceptable to the business to perform database backups once a day, depending on the volume of transactions.

3-6 A. A project timetable normally would not be found in a requirements document.

B. Assessing the vendor's quality processes would come after the requirements have been completed.

C. The decision to purchase a package from a vendor would come after the requirements have been completed.

D. The purpose of the requirements phase is to specify the functionality of the proposed system; therefore, an IS auditor would concentrate on the completeness of the specifications.

3-7 **A. With a purchased package, the design and development phases of the traditional life cycle have become replaceable with selection and configuration phases. A request for proposal from the supplier of packaged systems is called for and evaluated against predefined criteria for selection, before a decision is made to purchase the software. Thereafter, it is configured to meet the organization's requirement.**

B. The other phases of the system development life cycle (SDLC) such as feasibility study, requirements definition, implementation and post-implementation remain unaltered.

C. The other phases of the SDLC such as feasibility study, requirements definition, implementation and post-implementation remain unaltered.

D. In this scenario, the design and development phases of the traditional life cycle have become replaceable with selection and configuration phases.

3-8 A. Quality assurance has its focus on formal aspects of software development such as adhering to coding standards or a specific development methodology.

B. To fail at user specifications implies that requirements engineering has been done to describe the users' demands. Otherwise, there would not be a baseline of specifications to check against.

C. **Obviously, project management has failed to either set up or verify controls that provide for software or software modules under development that adhere to those specifications made by the users.**

D. A failure to meet user specifications might show up during user training or acceptance testing but is not the cause.

3-9 A. Because the other elements do not need to change, the integrity risk is not increased.

B. Because the other elements do not need to change; the concurrency risk is not increased.

C. Because the other elements do not need to change, the confidentiality risk is not increased.

D. The main change when using thin client architecture is making the servers critical to the operation; therefore, the probability that one of them fails is increased and, as a result, the availability risk is increased.

3-10 **A. Control totals built into the trailer record of each segment is the only option that will ensure all individual transactions sent are received completely.**

B. A log of the number of messages received provides supporting evidence, but their findings are either incomplete or not timely.

C. An electronic audit trail provides supporting evidence, but their findings are either incomplete or not timely.

D. Matching acknowledgment transactions received to the log of electronic data interchange (EDI) messages sent provides supporting evidence, but their findings are either incomplete or not timely.