Auditor's Guide to IT Auditing, Second Edition
By Richard E. Cascarino

APPENDIX B

Audit Program for Application Systems Auditing

THE BUSINESS SYSTEM is an integral element of the business function. Therefore the application and functional risks and the related controls must be considered together.

The approach selected to review business systems must address all relevant risks, management and general controls, and manual controls that are part of the business function under review.

There is a definite trend toward the migration of controls from the application to the general environment. For example, the database management system features may be used to restrict access to critical functions across applications.

An audit of general information technology (IT) control functions provides information on the reliability of the control structure, which could significantly impact the level of testing required during application-system audits.

Auditors need to have a full understanding of the technology platform that supports the application: database management systems, networks, security provisions, hardware, software, and operating systems.

To determine the effectiveness of access controls, the auditor should understand the capabilities and characteristics of the software, the manner in which the software is implemented from a technical point of view, the interrelationship of the application with other applications, systems software in use and conditions that allow overrides of controls, and the administrative controls related to the use of the access control software.

Application controls are dependent on the general controls in the IT environment. The general controls environment must be reviewed to ensure that controls resident in an application system cannot be circumvented by non-application system components.

General IT controls include, but are not limited to, data and program security, program-change control, system-development controls, and computer-operations controls.

Of major importance is the segregation of duties in terms of functional responsibilities as well as access to application system processing capabilities.

GENERAL AUDIT PROGRAMS FOR APPLICATION SYSTEMS

Questions	Yes	No	N/A	COMMENTS
Input Controls:				
Determine that appropriate input controls are used to ensure accuracy and completeness of data. Evaluate the effectiveness of various input controls in fulfilling their objectives.				
Audit Procedures:				
Check digit verification ensures accuracy of the data entered. The check digit is created as the result of a calculation routine. • Review the source code to ensure that the defined edits are included and are coded properly to achieve the desired result. • Review test results performed by the auditor as the system is being developed or modified. • Input test transactions with invalid numbers into an audit copy of the production software used to perform the check digit verification. The testing should be done in the test environment separate from the production environment. • Review error reports produced by the application to verify that errors are being detected. *Reasonableness and data validity edits ensure that the data is reasonable for the purpose intended. Some examples of edits include alphanumeric check, range of values check, and so on.* • Review the source code to ensure that the defined edits are included and are coded properly to achieve the desired result. • Review test results performed by the auditor as the system is being developed or modified. • Create test transactions to test edits of control significance. • Review edit reports from the production-processing system to verify that input errors are being detected.				
Hash total verification verifies accuracy for non-amount or non-numeric data. • Independent testing of a copy of the production software using copies of production data files as input to the test. The test should include steps to ensure that added, deleted, and/or modified records are properly detected by the verification routines. • Simulation of a hash total routine using independent audit software. Copies of production data files should be used as the test input.				

Questions	Yes	No	N/A	COMMENTS
• Manually re-foot hash totals from printouts of input data files produced by utilities program.				
Batch balancing verifies input to pre-established control total and item counts. *Note: Many applications provide manual override capabilities that allow for bypassing batch-balancing errors. It is necessary to review control over the use of this capability.* • Independent testing of a copy of the production software using copies of production data files as input to the test. The test should include steps to ensure that added, deleted, and/or modified records are properly detected by the verification routines. • Simulation of the routine using independent audit software. Copies of production data files should be used as the test input. • Manually re-foot totals from printouts of input data files. The printout can be obtained through standard utilities. • Observe balancing procedures.				
Observe data-entry operation to determine if screen masking is used to prevent confidential data from being displayed on a terminal screen during the inputting process.				
Review a sample of the transactions on the log to determine that a record is kept showing the individuals who input the data.				
Input verification can be performed by having a second individual review the data entered. Proper implementation of this control in conjunction with access controls can provide for the necessary separation of duties between the input and verification process. • Review access control rules for access to the input and verification transactions to ensure proper separation of duties. • Review control over the capability to override or bypass verification. Determine how the capability is installed and what authorization is required to use it.				
Call-back and dial-back to a predefined phone number. Verify the accuracy of the source attempting to initiate a transaction. • Initiate test transactions from an unauthorized location in the test environment. • Observe the call-back/dial-back procedures. • Analyze application software and hardware. • Review call-back/dial-back records.				
Input source verification provides assurance that data is only being modified by, or disclosed to, authorized individuals at known locations during approved time frames. Many applications provide this type of control by defining users, terminals, and printers in a security table that is embedded in the application software or data and is maintained by the application owner.				

Questions	Yes	No	N/A	COMMENTS
• Review on-line copy of the security table for propriety.				
Observe the operation to determine if the data-encryption method is used to prevent unauthorized disclosure and modification of data.				
A transaction log provides an audit trail for transactions processed. It may be a stand-alone log or it may be included as part of an overall system log. The log should be accurate and complete. • Use audit software developed specifically to read the log to get a report listing the totals and details of all transactions processed for the day. The totals can be matched to accounting entries. Differences between the records indicate potential problems.				
Run-to-run reconciliation ensures that the established control is maintained each time the data file is used for processing. • Use an independent software test. • Review outputs. • If the override capability is provided, additional review must be performed to ensure that the use of this capability is properly restricted and recorded on an audit trail.				
Reject re-entry data verification ensures correction and re-entry of rejected transactions. When items are rejected, a record or log of these items should be created so that correction and processing can be monitored. Records of outstanding rejected data and suspense items are reviewed regularly and followed up so that timely corrective action is taken and transactions are recorded in the correct period. • Observe reject re-entry operation. • Use an independent software test. • Review aging report of outstanding rejected items.				
Is there a complete and current set of documented procedures? • Interview employees. • Observe compliance with procedures. • Review documentation. • Review the procedures for updating documentation.				
A review of software modification controls could be performed as part of a business area audit if it is directed at reviewing user involvement in the software-modification process. The review could be used to assess user involvement in: • Authorization and approval of software-modification requests. • Providing user acceptance testing of software modifications. • Establishment of communications between the users and developers.				
Provisions for the backup and recovery of application data protect against unnecessary delays in providing required services.				

Questions	Yes	No	N/A	COMMENTS
• Review audit work performed by auditors conducting the system-development review to determine the extent of reliance that can be placed on the work. • Execute an independent test of backup and recovery of the application data. • Determine the extent of backup and recovery testing that was performed through a review of or participation in the implementation testing performed. If sufficient testing was performed to satisfy current audit objectives and assurances can be made that backup and recovery process has not changed since it was tested, reliance can be placed on the implementation testing rather than conducting another test.				
Business System Processing Controls:				
Determine that appropriate processing controls are used to ensure accuracy, completeness, and timeliness of data processed. Evaluate the effectiveness of various processing controls in fulfilling their objectives. Some of the commonly used audit techniques include: • Use simulated transactions to test processing logic, computations, and control programs in the application. If test transactions are prepared in accordance with user procedures, test data analysis can help the auditor to evaluate these procedures. It can also be used to evaluate individual programs or an entire system. It can direct the auditor to areas where erroneous processing has occurred especially when used in conjunction with data retrieval and program analysis techniques. Test data can be prepared by creating inputs, copying existing master records onto a test master file, or selecting live transactions. • Use specialized audit software to analyze the flow of data through the processing logic of the application software and document the logic paths, control conditions, and processing sequences. These techniques analyze the systems command language of job-control statements and the programming languages for the application. • Software mapping analysis can be used to review for non-executable codes in software. It documents all the codes in a given application and identifies the use of key data elements. • The snapshot audit technique is an automated tool used to trace a specific transaction through software and to document logic paths, control conditions, and processing sequences. This technique can verify program logic flow and help the auditor understand the various processing steps within the application software. Snapshot analysis employs a special code in the transaction record that triggers the printing of the record or data in question to a report format for further analysis. Specific instructions must be written into the application program to generate snapshot reports.				

Questions	Yes	No	N/A	COMMENTS
• The purpose of tracing is to document and analyze the logic paths in complex software. The objective of the tracing audit technique is to verify compliance with specifications, policies, and procedures by documenting how the application software processes transactions. By analyzing the transaction's path through the application, tracing can show instructions that have been executed and the sequence in which they have been executed. Tracing can also be used to verify omissions. Once the auditor understands the instructions that have been executed, analysis can be performed to determine whether the processing steps conform to organizational procedures, policies, and processing rules. Transaction tracing may be used to review transaction types and user identification numbers. • An integrated test facility (ITF) permits the internal auditor to examine an application in its normal operating environment. It involves entering and processing selected test transaction input into a live production system simultaneously with live data, tracing the flow of transactions through the various functions in the system, and comparing the actual results of the test transactions with predetermined or pre-calculated results. ITF can be used to test controls and processing of larger automated applications when it is not practical to process test data separately. Test data analysis/ITF may be used for transaction activity simulation, testing edit and validation criteria, testing of database updates and creation of computer-generated transactions, and testing of system output. • Embedded audit data collection is similar to continuous control monitoring and uses one or more specially programmed software subroutines embedded in the application software to screen and select input and computer-generated transactions. Distinct from other audit techniques, the method uses in-line code, whereby the application software collects the audit data while it processes data for production purposes. Activity monitoring, sampling, and exception reporting are all controlled by the subroutine parameters. The design and implementation of an embedded audit data-collection application is normally performed as an integral part of the system-development process. As continuous monitoring techniques are refined through use they alert management and auditors to actual or potential problems promptly. • Transaction retrieval and analysis are the primary automated tools designed to capture transactions for manual or automated verification analysis. They monitor activity and select transactions using error-based, parameter-based, or sample-based criteria. They are used in compliance testing to monitor transaction processing and to select data for verification.				

Questions	Yes	No	N/A	COMMENTS
• The code-comparison audit technique can be useful in evaluating software maintenance procedures, program library procedures, and program change controls. The auditor compares two versions of application software to identify any changes that have occurred since the earlier version was made and then analyzes the documentation that was prepared to authorize and execute the changes. The technique is used primarily to disclose unauthorized program changes. Either source or object code can be used for comparison. Comparison software can be purchased or developed. The software compares the application code and identifies inconsistencies between the two versions.				
Audit Procedures:				
Programmed cut-off controls prevent improper cut-off and reduce the risk of transactions being recorded in the wrong period; for example, an embedded calendar table can be used to compare with transaction dates or provide exception reporting of cut-off discrepancies. • Review source codes. • Review outputs.				
Cycle processing controls compare pre-established control totals of critical input fields to output totals accumulated by the system.				
• Review source codes. • Review outputs.				
Session controls are performed by the application software and designed to emulate a batch procedure. Totals of critical fields by type of transaction are automatically accumulated during a data-entry session and held for subsequent comparison with updated balances. • Review source codes. • Review outputs.				
File footings are software routines embedded into the application software that verify the dollar values and record counts or any other control fields of an application data file. It provides a primary control against inaccurate/incomplete data and a secondary control over unauthorized modification of application data. File footing is a detective control rather than a preventative control. • Develop audit software that performs the same computation.				
Independent confirmation letter is a control to ensure data accuracy. • Use software developed and maintained by audit to run confirmation letters and send to independent parties for verification.				
Piece count verification of valuables (i.e., securities) ensures the accuracy of computerized data. • Use audit-controlled software to produce count sheets. The assets are verified against the computer records.				

Questions	Yes	No	N/A	COMMENTS
Automated activity log records all activity within an application system. • Review application software source code. • Review the logs against a list of transactions processed. • Use audit software to verify the accuracy and completeness of the automated application log.				
Calculation simulation is a control when performed by a user. • Review source codes. • Use audit software to re-compute. • Manually re-compute.				
On-site and off-site backup of application data and software. • Define all the data and software that comprise the application. • Verify that copies of this data are created for backup storage for both on-site and off-site storage. • Evaluate the ability to meet the processing requirements of the application with the back-up data created. • Verify that required copies of back-up data and software are kept at each required location for the proper period of time.				
Restart and recovery procedures are the steps to reinitiate an application after a failure. For most database applications the restart and recovery is controlled by the database software. Most testing of the procedures is done as part of the installation test. The loss of transactions before processing is completed can be especially serious when data are entered in an interactive mode and in systems that use immediate update processing. • If the restart and recovery procedures were tested during the installation of the application, review the testing performed. • If the application is a database application and the restart and recovery is provided through the database software, they may have been tested as part of the database restart and recovery procedure testing. Review the test results to determine if they satisfy the application test objectives. • If there have been recent occasions to use restart/recovery procedures, review the results and determine the adequacy of the procedures employed. • Conduct independent tests in the test environment. • Determine if shadow file processing is used. This technique involves creating duplicate transaction records that are stored on a different device or, in some cases, at another location for recovery purposes.				
File-level encryption protects data from unauthorized disclosure and modification. It scrambles the data stored on an application file using a pre-determined key. • Execute software utility that will dump a few records of the encrypted file and verify that the printed data is encrypted.				

Questions	Yes	No	N/A	COMMENTS
• Review the management of encryption keys and encryption terminal definitions.				
File integrity routines independently verify that only acceptable data is maintained on a computer resident file. Edit criteria can be used as specifications for scanning the file to ensure that program edits have not been circumvented. • Use audit software or other programs that have built-in functions that perform frequency distributions on specified fields. Very high or very low occurrence can indicate potential problems and trigger follow-up.				
Having current and complete processing documentation helps ensure that operations are conducted in the correct and authorized manner. • Interview employees. • Observe compliance with procedures. • Review documentation. • Review the procedures for updating documentation.				
Transaction sequence verification ensures that all transactions entered have been processed. • Review output from the production system. • Review source codes. • Test transaction sequence verification software.				
Run-to-run reconciliation ensures that the established control is maintained each time the data file is used for processing. • Use an independent software test. • Review outputs. • If the override capability is provided, determine that the use of this capability is properly restricted and recorded.				
Controls over system-generated data are incorporated into systems that automatically generate transactions or perform calculations that are not subjected to human review. These controls validate the integrity and reasonableness of automatically generated transactions and reduce the risk of erroneous transactions (e.g., reports of such transactions or data may be produced for post-processing authorization, review, and reconciliation). Additional control over system-generated data occurs when there is a system-to-system interface that includes an automated comparison or reconciliation between the two discrete systems. • Review exception report. • Review source codes.				
Duplicate transaction testing ensures that the transaction has only been processed once. • Review output from the production system.				

Questions	Yes	No	N/A	COMMENTS
• Review source code used for verifying processing sequence. • Test transaction-sequence-verification software. • Review program source code used to identify and reject suspected duplicate transactions. • Conduct an independent test of the application software using copies of the production data and software in a test environment. • Review application edit reports that might highlight possible duplicate transactions.				
Programmed balancing controls are incorporated into the application software to ensure the accuracy and completeness of file update and report processing. The opening balance is checked against the closing balance from the previous cycle. The opening balance plus transactions processed equals the current closing balance. This control reduces the risks of processing with the wrong file, with incomplete or missing transactions, and with loss of file integrity. • Reconstruct account balances. • Review source codes.				
Override of computer edits involves intervention by the application owner by allowing the user the capability to bypass what under normal conditions would be an error that would prevent processing of the transaction to proceed. • Review the use of override to determine that it is restricted to an authorized user and that an audit trail of its use is properly recorded. Review the access/resource rules that control who can use the override capability.				
Software-modification controls are normally reviewed as part of a system-development project or as attention to the application-development function. A review of software-modification controls could be performed as part of a business audit if it is directed at reviewing user involvement in the software-modification process. The review could be used to assess user involvement in: • Authorization and approval of software modification requests. • Acceptance testing of software modifications. • Establishment of communications between the user and developers that assures user awareness and involvement in the software-modification process.				
File-label checking verifies that the files being used are correct. • Observe procedures. • Review source code. • Perform independent testing.				
Error reports highlight rejected transactions or errors.				
• Use test deck containing erroneous transactions • Review outputs.				

Questions	Yes	No	N/A	COMMENTS
Before/after change imaging.				
When application update programs change databases or application tables, a report of the before and after image of the changed data may be produced. Management can use this report to validate the integrity of the key application tables and databases. • Observe the operation. • Verify changes made to the tables and databases to the report generated by the update program.				
Data-transmission controls cause a proof calculation using a predefined algorithm to be performed on the information included in the transmission. The result of the proof total may be recorded on a header or trailer message segment prior to transmission. The same calculation is then performed when the message is received and the results are compared with information recorded on the header or trailer. If differences are identified, the sender is requested to retransmit the information. • Observe the operation. • Test the application in a test environment.				
Business System Output Controls:				
Determine that appropriate output controls are used to ensure accuracy, completeness, timeliness, and proper distribution of data processed. Evaluate the effectiveness of various processing controls in fulfilling their objectives.				
Review security software access control definitions, logon IDs and associated privileges, authentication methods, access and resource rules, source and shift group definitions, and logical transactional groups for appropriateness.				
Observe the operation and interview staff to determine that terminals are restricted to authorized personnel by these means: • Terminals are located in supervised and secured areas. • Physical identifiers such as cards or keys are required for terminal operation. Cards and keys are given to authorized personnel only. • Terminals are restricted for authorized functions.				
Online acknowledgment for automated output received. • Review source code for the specific application programs used to provide online acknowledgment. • Observe the operation to verify that online acknowledgment is being used and is working as it was intended. • Test the application in a test environment.				
Edit to ensure all hard-copy output is produced. • Review hard-copy output from production process.				
Questions	**Yes**	**No**	**N/A**	**COMMENTS**
• Observe distribution of output.				

Controlled distribution of hard-copy output. • Observe manual distribution process. • Review application job control language (JCL) to identify destinations for all outputs that are distributed automatically. *Input to output reconciliation controls.* • Obtain prior day's ending balance and add and subtract the current day's activity to arrive at ending balance. Reconcile ending balance to output. • Perform input/output analysis by tracing transactions from initiation to the output phase. The approach relies heavily on the analysis of data and information rather than controls.				
Sensitive computer forms are controlled while in storage and in use. Forms are pre-numbered and usage is accounted for in numerical sequence. • Verify that the current cycle's beginning number is one higher than the last cycle's ending number. • Re-compute the number of forms on hand. • Piece count the number of forms on hand. • Observe the operation.				
The output should contain descriptive headings for dates, numbered pages, and data classifications. • Review output.				
If an application maintains sensitive data, screen-masking controls should be employed. • Review output. • Observe operation.				
User review of computer outputs. • Observe the reconciliation procedures performed by the users. • Use audit software to re-create the computer-generated transactions that would serve as a basis for verification during the audit.				
Sensitive data destruction procedures provide for secure disposal of all sensitive outputs. • Walk through the department. • Observe the destruction process.				
Questions	**Yes**	**No**	**N/A**	**COMMENTS**
Application Access Controls:				

Information integrity may be impaired through the transaction processing functions of the application or through direct access to the application's data files or database. Control over the accurate updating of master file or database records is important. Anyone with direct access to master file modification functions (e.g., database utilities) may be able to circumvent established procedures for the initiation, approval, and recording of transactions or access to data and may possibly gain indirect access to assets.				
Information integrity is dependent on the overall data-access-control environment, controls internal to the application system, and access to the data. Access security over applications systems can be incorporated into the application or provided by access-control software; a database-management system or other software may provide some security functions. In addition to application software, there are three common types of systems software used to control access: teleprocessing monitors, access control software, and database management systems (DBMS) software. *Evaluate the effectiveness of access control to the application and its data.*				
Audit Procedures:				
Effective control over access to computer functions and related data is dependent on the use of the application's security features and/or access-control software. A database management system or other software also may provide some security functions. Access controls are designed to enforce the segregation of duties. *Review security packages access-control definitions, logon IDs and associated privileges, authentication methods, access and resource rules, source and shift group definitions, and logical transactional groups for appropriateness.*				
Observe the operation and interview staff to determine that terminals are restricted to authorized personnel by these means: • Terminals are located in supervised and secured areas. • Physical identifiers such as cards or keys are required for terminal operation. Cards and keys are controlled by authorized personnel only. • Terminals are restricted to authorized functions.				
Review approval forms to determine that access to data, terminals, and applications have been approved by data/application owners. • *Review violation reports to determine that exceptions have been resolved promptly.*				