nformation Systems Control Journal, Volume 5, 2002

IT Audit Basics

Auditing General and Application Controls

By S. Anantha Sayana, CISA, CIA

There are many areas and elements of information systems (IS) audit. Based on the scope of the assignment, the annual audit plan and other factors, the IS auditor may undertake the review of a specific area. (Refer to the "IT Audit Basics" column in *Journal*, volume 1, 2002, for the elements of IS audit.)

Auditing General Controls

A general controls review attempts to gain an overall impression of the controls that are present in the environment surrounding the information systems. These include the organizational and administrative structure of the IS function, the existence of policies and procedures for the day-to-day operations, availability of staff and their skills and the overall control environment. It is important for the IS auditor to obtain an understanding of these as they are the foundation on which other controls reside.

A general controls review would also include the infrastructure and environmental controls. A review of the data center or information processing facility should cover the adequacy of air conditioning (temperature, humidity), power supply (uninterruptible power supplies, generators) and smoke detectors/fire suppression systems, a conducive clean and dust free environment, protection from floods and water seepage as well as neat and identifiable electrical and network cabling.

Physical access control is another important area for review. Today in a highly networked world, logical access to computer systems is literally universal, yet there is a necessity to control physical access too. There are certain commands and settings that can be executed only from the console of the server and hence it is important to enclose all servers in a secure location protected by suitable mechanisms like locked doors, access swipe cards, biometric access devices or a combination of these. Further the IS auditors also should review the overall access control measures to the entire facility for controls like security guards at the entry gates, displaying of identification badges and logging visitor access.

Auditing Application Controls

Application Software

Application software is the software that processes business transactions. The application software could be a payroll system, a retail banking system, an inventory system, a billing system or, possibly, an integrated ERP (enterprise resource planning) system. It is the application software that understands data with reference to their business context. The rules pertaining to the business processes are implemented in the application software.

Most users interact with the computer systems only through the application software. The application software enables and also limits the actions that a user can do.

It is very important to subject application software to a thorough audit because the business processes and transactions involving money, material and services flow through the application software package.

Approach to Auditing Application Software

The first question to ask in an application software review is, "What does the application software do; what business function or activity does it perform?"

In this context it is very necessary for the IS auditor to know the business. For application reviews, the IS auditor's knowledge of the intricacies of the business is as important, if not more so, as the technical knowledge. Hence the first step in an application review is to understand the business function/activity that the software serves. This can be done through the study of the operating/work procedures of the organization or other reference material. The other alternative is by interviewing the personnel.

Once this is done, it is necessary to identify the potential risks associated with the business activity/function served by the application (what can go wrong?) and to see how these risks are handled by the software (what controls it?).

Application Software Audit Methodology

The information systems audit of application software should mainly cover the following areas:

- Adherence to business rules in the flow and accuracy in processing
- Validations of various data inputs
- Logical access control and authorization
- Exception handling and logging

The steps to be performed in carrying out an application software review are as follows:

- Study and review of documentation relating to the application. However, the IS auditor may find situations in real life where documentation is not available or is

not updated. In such cases, the auditor should obtain technical information about the design and architecture of the system through interviews.

- Study key functions of the software at work by observing and interacting with operating personnel during work. This gives an opportunity to see how processes actually flow and also observe associated manual activities that could act as complementary controls.
- Run through the various menus, features and options to identify processes and options for conformance to business rules and practices. (Studying the documentation before this can significantly hasten the activity.) To illustrate with an example, it is a well accepted rule in financial accounting that once an accounting transaction has been keyed in and confirmed on the system to update the ledgers it should not be edited or modified. The correct method would be to pass a fresh reversal transaction to correct errors, if any. However, if the IS auditor observes that there is an option in the software to "edit/modify transactions," this would be noted as a control deficiency for correction.
  This kind of run-through can be done more effectively if a development/test system is made available to the IS auditor. In the absence of such a facility, the auditor only can watch the system run by the system administrator and make notes. The auditor is advised not to do any testing on a production system as this could affect adversely a "live" system.
- Validate every input to the system against the applicable criteria. Such validations go a long way in eliminating errors and ensuring data integrity. Apart from simple validations for numeric, character and date fields, all inputs should be validated with range checks, permissible values, etc. Validation checks that are built on application-specific logic can act as powerful controls not only for ensuring data accuracy but also to prevent undesirable data manipulations. The IS auditor can check validations by actually testing them out in the development/test system. Alternatively, looking at the database definitions, the associated triggers and stored procedures would be the way for a technically savvy IS auditor to review the validations.
- Verify access control in application software. This consists of two aspects--the inherent design of the access control module and the nature of access granted to various users and its maintenance. Every application software has a number of modules/options/menus that cater to the different functionality provided by the software. Different users will need access to various features based on their responsibilities and job descriptions. All access should be strictly based on the need to know and do. The design of the access control module may be of varied types. Most software would check a combination of user id and passwords before allowing access. Access may be controlled for each module, menu option, each screen or controlled through objects. Often the matrix of users versus the options/actions becomes too large and complex to maintain hence it is normal to define certain roles for different classes of employees and group them together and assign them similar access. The IS auditor should review the design of the access control module keeping in mind the criticality of the functions/actions possible in the software and evaluate whether the design provides the level of control and granularity to selectively and strictly allows access as per the job

requirements of all the users.

Having done this, the auditor should proceed to verify whether all existing users have appropriate access as evidenced by their job descriptions and whether access to certain critical activities are allowed only to select personnel duly authorized. It also is necessary to verify who has administrator/superuser rights and how such rights are used/controlled. Ideally no one in the IT/development group should have any access to the production data. All actions on the data by the superuser should be logged and verified by the data owners regularly.

- Verify how errors and exceptions are handled. In many activities software provides options and ways to reverse transactions, correct errors, allow transactions under special circumstances, etc. Each one of these is special to the business and based on the rules and procedures defined by the organization for these. The IS auditor needs to see how the software handles these. Are these circumstances properly authorized in the software? Does it capture the user id and time stamp for all transactions to provide suitable trails? Are the exceptions and critical activities like updates to global parameters logged for independent review later?
- Correct any weaknesses found at the end of an applications review in the software that could lead to errors or compromises in security. These would need to be corrected by either changes in design and/or some recoding. While this would be addressed by the IT department, the user or owner of the application from the functional area would want to know if any of these weaknesses have been exploited by anyone and whether there have been any losses. To provide an answer to this question the IS auditor should download all the data for the period in question and run a series of comprehensive tests using an audit software and determine if any error or fraud really occurred or not.
- Evaluate the environment under which the application runs. The audit of the application software alone is not enough. Generally, it is prudent to conduct a security review of the operating system and the database in which the application runs while doing an application review.

All critical applications used in an organization need to be subjected to detailed review by an IS auditor. This is one of the most important aspect of IS audit for a business. The job of application review becomes more complex as the application becomes larger and integrated. While auditing complex applications, it is always good to start with a generic industry-based template of an audit work program and slowly customize the work program to the specific situation as the audit progresses.

The IS Auditing Guideline issued by ISACA® on *Application Systems Review under Performance of Work* contains detailed guidelines on planning the review, application risks, documenting the flow of transactions, and identifying and testing the application system controls and reporting. The matter contained in these guidelines have not been reproduced in this article but can be invaluable for an IS auditor seeking guidance or clarifications on application reviews. The guidelines can be seen on ISACA's web site, www.isaca.org, under standards.