PART ONE

Conducting an Information Systems Audit

CHAPTER ONE

1 Overview of Systems Audit

IN THIS CHAPTER WE discuss why an information systems audit would be conducted. The chapter also identifies the challenges that an auditor will face while auditing a computerized system. Critical differences between computerized and noncomputerized systems have also been identified. Upon completion of this chapter, the reader will have an understanding of the salient features of a computerized system that an information systems auditor must keep in mind.

INFORMATION SYSTEMS AUDIT

An information systems audit is an examination of various controls within an information systems infrastructure. It is the process involving collection and evaluation of evidence of the design and functions of controls designed and implemented in information systems, practices, and operations. The auditor, subsequent to evaluation of the evidence, forms an opinion on whether the information systems safeguard assets, maintain data integrity, and operate effectively and efficiently in order to achieve the agreed-upon goals and objectives of the entity. An information systems audit can

be performed independently of or along with an audit of financial statements. More often than not, it remains an independent function used during testing of controls.

INFORMATION SYSTEMS AUDITOR

Under the existing practices in various countries, any person having a recognized qualification in information systems audit can conduct an information systems audit. To be a recognized qualification, it must be awarded by an institution that is acknowledged by the laws of the country. These institutions can be academic or professional bodies. The qualification can also be designated by membership of an association or body of person on the basis of their internal norms of qualification for such membership. Usually such membership is renewable annually by paying a membership fee. Qualifications from academic institutions usually do not involve any recurring membership cost. It is important to note whether the regulatory authorities recognize the qualification of an information systems auditor for conducting an information systems audit in a specific country. Industries are free to recognize qualifications awarded by institutions other than those mentioned earlier.

It may be noted that, unless specified by the auditee or regulatory authorities, there is no requirement of any additional qualification other than that of an information systems auditor, in order to conduct an information systems audit.

LEGAL REQUIREMENTS OF AN INFORMATION SYSTEMS AUDIT

More often than not, an information systems audit is a best practice or an ethical exercise rather than a legal requirement. However, the audit may be legally required in some countries, such as under the Sarbanes-Oxley Act of 2002 in the United States.

Major requirements of the Sarbanes-Oxley Act with relation to information systems audit are provided in the following sections.

The Sarbanes-Oxley Act of 2002

The Sarbanes-Oxley Act came into force in 2002 to ensure better regulation of financial practices and corporate governance and requires a number of compliances. The act is named after Senator Paul Sarbanes and Representative Michael Oxley, who were its main architects.

Form 10-K

Form 10-K is the name of the form that every domestic issuer in the United States has to submit to the Securities and Exchange Commission. The form provides

a comprehensive overview of the business of the filer, along with the business's financial condition and audited statements.

Securities and Exchange Commission

Better known by its acronym, SEC, the Securities and Exchange Commission is the apex regulator responsible for enforcing all of the laws and regulations of the securities industry in the United States.

1. Section 302 assigns corporate responsibility for accuracy of financial statements and operational activities to the chief executive officer (CEO) and chief finance officer (CFO). The signing officers certify that they have reviewed the reports and that they are free of untrue statements, material omissions, or misleading statements. This can be assured only if an information systems audit has reviewed the operation of the software and systems involved in producing the financial statements.
2. Section 404(b) calls for certification from auditor on management assessment of internal control. The assessment seeks to ensure that adequate controls are established and maintained for financial reporting. Naturally an information systems audit is useful for such an assessment.
3. Section 409 requires immediate disclosure of changes in financial position and operations in real time. An information systems audit can assess the readiness of an organization in this regard.
4. Section 802 requires retention of electronic records that have an impact on assets or performance of a company. An information systems auditor reviews the preparedness of any organization to prevent willful or accidental destruction of such records.

Following is a sample certification from the 10-K filing of Kraft Foods Inc. with the Securities and Exchange Commission.

CERTIFICATION

I, Irene B. Rosenfeld, certify that:

1. I have reviewed this annual report on Form 10-K of Kraft Foods Inc.;
2. Based on my knowledge, this report does not contain any untrue statement of a material fact or omit to state a material fact necessary to make the statements made, in light of the circumstances under which such statements were made, not misleading with respect to the period covered by this report;

(*Continued*)

3. Based on my knowledge, the financial statements, and other financial information included in this report, fairly present in all material respects the financial condition, results of operations and cash flows of the registrant as of, and for, the periods presented in this report;
4. The registrant's other certifying officer(s) and I are responsible for establishing and maintaining disclosure controls and procedures (as defined in Exchange Act Rules 13a–15(e) and 15d–15(e)) and internal control over financial reporting (as defined in Exchange Act Rules 13a–15(f) and 15d–15(f)) for the registrant and have:

   Designed such disclosure controls and procedures, or caused such disclosure controls and procedures to be designed under our supervision, to ensure that material information relating to the registrant, including its consolidated subsidiaries, is made known to us by others within those entities, particularly during the period in which this report is being prepared;

   Designed such internal control over financial reporting, or caused such internal control over financial reporting to be designed under our supervision, to provide reasonable assurance regarding the reliability of financial reporting and the preparation of financial statements for external purposes in accordance with generally accepted accounting principles;

   Evaluated the effectiveness of the registrant's disclosure controls and procedures and presented in this report our conclusions about the effectiveness of the disclosure controls and procedures, as of the end of the period covered by this report based on such evaluation; and

   Disclosed in this report any change in the registrant's internal control over financial reporting that occurred during the registrant's most recent fiscal quarter (the registrant's fourth fiscal quarter in the case of an annual report) that has materially affected, or is reasonably likely to materially affect, the registrant's internal control over financial reporting; and
5. The registrant's other certifying officer(s) and I have disclosed, based on our most recent evaluation of internal control over financial reporting, to the registrant's auditors and the audit committee of the registrant's board of directors (or persons performing the equivalent functions):

   All significant deficiencies and material weaknesses in the design or operation of internal control over financial reporting which are reasonably likely to adversely affect the registrant's ability to record, process, summarize and report financial information; and

   Any fraud, whether or not material, that involves management or other employees who have a significant role in the registrant's internal control over financial reporting.

Date: February 28, 2011
/s/ IRENE B. ROSENFELD
Irene B. Rosenfeld
Chairman and Chief Executive Officer

The audit under Statement on Auditing Standards (SAS) No. 70, developed by the American Institute of Certified Public Accountants (AICPA), is another example of statutory and quasi-statutory needs to perform information systems audits.

Statement on Auditing Standards

Usually referred to as SAS, these standards narrate generally accepted auditing practices that an auditor should follow while conducting an audit and issuing the audit report. These are issued by the Auditing Standards Board of the American Institute of Certified Public Accountants in the United States. Most countries have their independent accounting and auditing body, which issues such standards.

The standard identifies the factors that an independent financial auditor of an organization should consider when auditing the financial statements of an entity that uses a service organization to process certain transactions. Since the evaluation is based essentially on examination of the controls employed by the service organization, an information systems audit will be found extremely useful.

Though there may not be any specific legal requirement of an information systems audit, more often than not a statutory financial audit requires testing of adequacy and efficiency of internal control before expressing an audit opinion. With most of the auditees having a computerized environment as one of their major logistics, and using integrated enterprise resources management software, it is imperative that an information systems audit is conducted to form an opinion on the adequacy of internal control.

SYSTEMS ENVIRONMENT AND INFORMATION SYSTEMS AUDIT

Computerization is a tool that gives organizations the capability to provide better customer service, to conduct better housekeeping, and so on, to enable optimization of the use of resources. To ensure that computerization takes care of existing and emerging needs of the organization, the following nine issues must be considered:

1. Standardization of hardware, operating systems, system software, and applications: Failure to ensure such standardization creates complex technology management issues, which often manifests through involvement of multiple systems in a single process instead of an integrated process ensuring nonduplication of functions.
2. Use of software to facilitate interconnectivity of systems intensifies the need for a systems audit to ensure that information flow is smooth and not compromised.
3. The need for high levels of security not only calls for technical competence but also requires continuous testing of efficiency and searching for new, emerging vulnerabilities as well.

4. Communication and networking involving the use of networks facilitate establishing a centralized database and distributed processing on one hand, but on the other hand expose the entity to the risk of security breach from multiple sources. Consequently the scope of a systems audit enlarges and involves more complex testing.
5. A technology infrastructure with periodic up grades often leads to migration from one system to another. The information systems audit is required to keep pace with not only the technology but also the maturity of the organization. A more matured organization entrusts more critical resources to the information system and at the same time becomes more susceptible to a systems breach.
6. The need for business process reengineering is a consequence of the evolution of business complexity, which necessarily calls for an enlarged role of the information systems. Such reengineering brings about serious challenges to smooth migration and maintenance of data integrity.
7. Issues of human relations in a computerized environment are perhaps one of the greatest challenges for an information systems audit. Unpredictable and indispensable as they are, human resources define the fine line differentiating the success or failure of an information technology project. The information systems auditor finds the task of assessing adequacy and efficiency of such controls extremely difficult and often subjective.
8. Sharing of technology experiences between organizations and between various levels of an organization enriches the quality of performance as it ensures that the same mistake is not repeated twice. The comfort level of an information systems auditor is greater in an organization that enables a system of internal learning.
9. An information systems audit assumes greater importance in the face of the increased use of credit and debit cards and e-commerce interface in the regular functioning of an entity. These are activities that require closer monitoring as well as the assurance that the access and security aspects of these systems are well laid out.

An information systems audit ensures that the computerization activity of an entity follows the best practices and abides by all statutory and quasi-statutory requirements in its quest to achieve the objective of computerization.

The scope of an information systems audit extends over all information systems assets and processes that are owned or used by an entity or its representatives. An information systems audit seeks to ensure that the confidentiality, integrity, and availability of all information systems assets and processes are not compromised. In order to achieve this, an information systems audit focuses on the existence, adequacy, and efficiency of relevant controls.

INFORMATION SYSTEMS ASSETS

Information systems assets may be segregated into various kinds, such as:

- **Information assets:** These include databases, data files, system documentation, operating manuals, training guides and materials, operational and support

guidelines, continuity plans, backup guidelines, archived information, and so on. More often than not, values of these assets are utilitarian and rules of physical valuation are not applicable on them.

- **Software assets:** These include operating systems, application software, system software, development tools, implementation and monitoring utilities, and so on. Essentially these are tools that enable data processing, information generation, and reporting.
- **Physical assets:** These include, among others, the following devices:
  - Computer equipment: processors, monitors, laptops
  - Communications equipment: routers, fax machines, answering machines, IP phones
  - Storage media: magnetic storages, pen drives
  - Other technical equipment: power supplies, including power backup, temperature and humidity control devices, furniture, accommodation, and so forth
- **Services:** These include computing services, interoffice and intraoffice communications services, and general utilities, for example, heating, lighting, power, and temperature control. The increased popularity of cloud computing is redefining various software and physical assets as cloud services wherein the software, processing power, and storage are all provided by a cloud computing service provider.

Cloud Computing

Cloud computing is a shared service that provides computing power inclusive of processor, software, storage space, and so on for hire. The user connects to the service through a network, usually based on the Internet. This converts computing from a product-based solution to a service and allows the user to save on procurement cost and have anywhere access.

CLASSIFICATION OF CONTROLS

Controls are central to the idea of an information systems audit. They define a point of action in a work process wherein a decision to select the subsequent action arises. Controls without an alternative are fictitious controls that exist only on paper without any impact potential.

Controls can be classified in different ways. Three basic categories are general controls, application controls, and objective-based control classification, which are discussed in the following sections.

General Controls

General controls are basic hygiene issues that any system should observe. These are applicable across all systems though the extent of application along with segmental

importance may vary. General control features in most systems can be classified into the following six categories:

1. **Organization and operation controls**, which include:
   a. Segregation of functions between the information technology department and users
   b. Provision for general authorization over the execution of transactions, for example, prohibiting a person from initiating and authorizing transactions
   c. Segregation of functions within the information technology department
2. **Systems development and documentation controls**, which include:
   a. Process of review, testing, and approval of new systems as well as modified systems
   b. Control over program and parameter changes
   c. Documentation procedures
3. **Hardware and system software controls**, which include:
   a. Automatic error detection features
   b. Periodic preventive maintenance
   c. Formal procedures to recover from hardware errors
   d. Adequate authorization and control over implementation of, and changes to, operating systems software
4. **Access controls**, which are designed:
   a. To prevent and alert unauthorized access to any information system asset
   b. To prevent deliberate or accidental errors that may be caused by improper alteration of data files or by unauthorized or incorrect use of computer resources, including software
   c. To establish a robust layered authentication scheme for third-party resources being hosted by the organization, more specifically, in cases of cloud computing
5. **Data and procedural controls**, which include:
   a. A control or balancing function
   b. Written manuals in support of systems and procedures
   c. Capability to restore or replace lost, damaged, or incorrect data files
6. **Business continuity controls**, which include:
   a. A control to detect, alert, and act on identification of threats to business continuity
   b. An established plan to ensure earliest resumption of most critical functions of information technology department

Application Controls

The detailed structure of application controls will depend on the nature of the application. Broadly there are three types of application controls appropriate to any application. These are:

1. **Input controls**, which include control over:
   a. Transaction entry
   b. File maintenance transactions

   c. Inquiry transactions
   d. Error correction transactions
   e. System-induced transactions
2. **Processing controls**, which are usually included in application programs and designed to prevent or detect errors of the following nature:
   a. Failure to process all input transactions, or erroneous processing
   b. Duplicate processing or updating wrong file or files
   c. Processing inputs that are either illogical or unreasonable
   d. Loss, unintentional modification, or distortion of data during processing
3. **Output controls,** which are used to assure the accuracy of processing results, and to ensure that only authorized personnel receive the output. The basic output controls are:
   a. Balancing
   b. Visual scanning or verification
   c. Distribution
   d. Storage, retrieval, and distribution

Objective-Based Control Classification

The classification of controls on the basis of action or objectives would lead to the following five categories:

1. **Directive controls:** These controls comprise management actions, procedures, directives, or guidelines that facilitate the occurrence of a preferred event. Such controls influence the entire system or operation and address areas of usage, maintenance, audit, control, and security attributes of a system and software with the object of ensuring integrity, reliability, and availability of systems resources.
2. **Preventive controls:** These controls aim to establish a reliable system and are based on standards, methods, practices, tools, and techniques. These controls could be automated or manual depending on whether human intervention is required to trigger the same. Preventive controls also act as a deterrent that minimizes the possibility of the occurrence of undesirable events, including computer-related fraud, theft, embezzlement, possible errors, omissions, and irregularities. These controls address various issues, including maintenance, security, usage, and control features of the system.
3. **Detective controls:** These controls are designed to detect variation outside control limits. They assess whether various controls (for example, directive or preventive) have achieved their objectives. These controls primarily focus on detection of errors, omissions, and irregularities. In addition, they also highlight system quality, controls, and security issues that need management intervention.
4. **Corrective controls:** These controls continue from the detections made by detective controls by making available information, procedures, and instructions for correcting identified errors, omissions, and noncompliances. Corrective control tools and techniques can be manual and automated. These controls highlight the usability of the system along with the availability of audit trails to conduct subsequent audits.

5. **Recovery controls:** These controls assume criticality in face of exposure to events that threaten a disruption in services. These controls describe and provide tools, techniques, and procedures of backup, restoration, recovery, and restart of an information resource. These controls define a formal structure to ensure availability of all required resources necessary to ensure an early recovery from disaster. These controls may be designed for a specific activity, an entire operation, or an entire organization. Recovery controls include timely backup and rotation of data and program files, checkpoints, restart/rerun procedures, record and file retention, and so forth. Depending on the organization structure and technology implemented, the grouping of recovery controls with corrective controls may facilitate better implementation.

THE IMPACT OF COMPUTERS ON INFORMATION

Not all controls that are useful in a noncomputerized system may be as useful or even necessary in a computerized system. Arguably the functional attributes of all such controls will be necessary, but technology interface may allow a combination of different functions within one control. In order to make a better assessment of controls that need to be replicated in a computerized system, it is important to understand the impact of computers on information as well as on information systems. The fact that changes in a processing system often obscure the need for implementing a control underscores the need to review the following subprocesses to recognize the transformation of a process. The following checklist of 13 items will also serve for reviewing a system that has migrated from one platform to another.

1. **Transaction initiation:** In a computerized system, many transactions may be initiated by the system itself. Thus all transactions may not have a supporting initiation document. A common example is execution of a standing instruction in banking software.
2. **Inputs:** Information may be committed directly into the system, without any hard-copy evidence. This is common in enterprise-wide integrated software wherein one input creates a chain of inputs in various subsystems, often after partial processing by a subsystem before onward processing. For example, computation of the cost of a product is influenced by a material receipt, as it changes the average issue price, which is a component of the standard cost of a product. Though no entry is directly being made in the costing module, entry in the inventory module has an impact on the costing module.
3. **Authorization:** Unlike a manual system, in which a supervisor reviews a transaction and then authorizes it, in a computerized system the authorization limits may be set within the system itself. Thus manual supervision may not be required. A common example is found in the operation of credit cards, where predetermined limits are set.

4. **Movement of documents:** In computerized systems, documents move electronically, including on e-mail or group documentation management systems. Cloud computing even takes physical custody of the documents out of the physical perimeter of the organization. Collaborative applications allow multiple users to access the same file and work on documents simultaneously. Exclusive custody of the document is no longer necessary, which creates a need to design specific controls to manage access and usage.
5. **Transaction processing:** In computerized application systems, processing is done electronically within the computer by programs that follow predetermined rules and consequently do not leave behind any physical audit trail. Thus there must be controls to test the processing, preferably before implementation of the software. Such controls need to be redesigned to assess processing efficiency post-implementation.
6. **Complexity of processing:** By using the high processing capabilities of computers, complex processing functions can be performed that are not possible in a manual system. Consequently, no controls were designed for such processes. In fact, the entire process has to be initiated specifically for the computerized system.
7. **Information storage:** Information may be categorized into two forms—permanent and temporary. Permanent information needs to be maintained for longer periods of time. Various backup facilities and storage media are available in computer systems, which raises a question of careful selection in light of the rapid progress in technology. Third-party storage services add to the list of alternatives available for storage. One of the critical issues involving choice of storage is the ability of future hardware to access the same. Often the storage media may remain uncompromised but the hardware required to retrieve data becomes obsolete. Floppy drives and cartridges are examples of such developments.
8. **Outputs:** Unless required legally or warranted by the workflow, printed output from system is actively discouraged. In many cases the output is in the form of visual displays, including e-mail and screen displays, which make evidence collection a specialized activity. The increased use of personal handheld devices has promoted ideas about generating output as text messages or e-mailing them as an attached document. These have since emerged as common output options.
9. **Filing of documents:** In a manual system, data and information stored in files can be manually retrieved whenever required. In a computerized system, data retrieval from the database requires either running the report generation again or using alternative techniques available for storage of reports. Use of data warehousing makes preprocessed or semiprocessed data available for faster retrieval. This effectively promotes the concept of separation of data and reports, enabling organizations to prevent data access whenever reports are required.
10. **Audit trails:** When the auditor traces a transaction from initiation to the final output, the flow of events is reconstructed. This function is aided by an audit trail. In a computerized system, the auditor needs to be familiarized with the processing rules because the processing path may not be externally observable, especially when processing is complex.

11. **Procedure manual:** Procedure manuals in a manual system help an auditor to know the steps required to process any transaction. In computerized systems, help menus and program documentation have to be looked into. The major problem faced in this regard is in updating the documentation, whenever the system is modified. Often there is a gap in this area, leading to a modified feature of the software being undocumented. This is a common weakness for customized solutions.
12. **Monitoring and supervision:** In a computerized system, a large part of the monitoring and supervision is done automatically and online by the system. Controls involving data editing, validation routines, and checks and balancing are often performed by the system itself. Consequently these checks need to be analyzed at the program level rather than at the operational level, where there may not be adequate evidence available. This becomes imperative when the processing is outsourced to locations that are not under the direct supervision of the information owner.
13. **Segregation of duties:** Segregation of duties tends to be compromised in a computerized system. Unless specifically designed, it is often possible for an individual to enter, change, and delete a transaction. This requires the introduction of compensating controls, including a supervisory review to ensure that concerned individuals discharge their responsibilities within the defined scope.

THE IMPACT OF COMPUTERS ON AUDITING

Much as computers have changed the way information is handled and stored, their use has also affected the process of auditing a company. Entities produce standardized information on a real-time, online basis. The scope of a financial audit has also migrated from essentially a "backward-looking" activity to an assurance service by which the subscribers seek to form an opinion about the sustainability of an entity.

Thus, in order to ensure the accuracy and relevance of financial figures being commented upon, one needs to understand the process of generation of the same. This involves the function of an information systems auditor. The areas where the financial auditor would concentrate depend greatly on the work of the information systems auditor, and may even require continued assistance, such as in the following activities:

1. **Computerized audit trail:** Paper-based trails as a mode of evidence collection is giving place to screen-based outputs and inputs. Audit trails are now design-dependent and not function-dependent.
2. **Interwoven complex systems:** In an integrated system consisting of a number of interacting subsystems, errors or irregularity in a subsystem can quickly propagate to another subsystem and cause material losses. The auditor needs to understand the referred loss potential of a control failure.

3. **Transaction walkthroughs:** An auditor would need to follow a transaction from its initiation to its end to get an understanding of the process flow. This will be useful to identify the system's strengths and weakness and plan subsequent audit tests.
4. **Entropy in complex systems:** Entropy is the tendency of systems toward internal disorder and eventual collapse. A computerized system is exposed to this threat because of various reasons, including changed business conditions, which can make existing information redundant, or multiply the volume of computations, or increase the difficulties in maintenance.
5. **Outsourced and distributed information systems:** A large number of activities are either outsourced or take place in geographically distributed facilities. Since physical presence at all facilities may not be possible to gather audit evidence, the auditor needs to understand the process flow and may be required to design audit routines to collect evidence and identify areas where errors and irregularities are likely to happen.

INFORMATION SYSTEMS AUDIT COVERAGE

As described earlier, an information systems audit would cover all information system assets and processes. In order to develop a comprehensive opinion about the occurrence or possibility of compromise of confidentiality, integrity, and availability of information system assets and processes, the auditor should be knowledgeable about the following nine aspects:

1. Hardware security issues
2. Software security issues
3. Information systems audit requirements
4. Conducting an information systems audit
5. Risk-based information systems audit
6. Auditing disaster recovery plans
7. Auditing in the e-commerce environment
8. Security testing
9. Information security grading, such as ISecGrade framework

These topics are discussed in detail in the chapters of this book. We have also included a case study on conducting an information systems audit at a bank branch. ISecGrade checklists have been provided.