Practical Approach to Information System Audit

A. Rafeq

< EXECUTIVE SUMMARY >

◆Is Audit is considered to be a subset of Internal Audit. The objective of IS Audit is ensuring that appropriate controls are implemented in IT as designed and envisaged by the senior management. IS Audit is expected to provide reasonable assurance to the management that appropriate controls are designed and implemented in Information systems supported by Information Technology. IS auditing involves finalizing scope of audit, identifying related standards, perform specific tasks and execute audit as per audit phases. Is Auditors have to understand the key concepts of IS risks, Risk management, IS security, controls, objective and the methodology of IS audit.

OVERVIEW

The overall approach of this article is to provide overview of Information Systems (IS) Audit. The article is not expected to be comprehensive in its approach on the subject but provides ideas which can be explored. This article explains key concepts and inter-relationships of information systems security, controls and its audit. It provides a sample listing of IS Audit assignments as relevant to banks and its branches.

NEED FOR IS AUDIT

IS Audit is not a mandatory requirement in India. It is considered to be a subset of internal audit. As in internal audit, the scope and objective are prescribed by the management of the company. The overall objective of internal audit is to ensure that appropriate internal controls are implemented within the enterprise as designed and envisaged by the senior management. Similarly, the overall objective of IS Audit is to ensure that appropriate controls are implemented in IT as designed and envisaged by the senior management. IS Audit is expected to provide reasonable assurance to management that appropriate controls are designed and implemented in the Information systems supported by Information Technology. IS Auditors have to understand the key concepts of IS Risks, Risk management, IS Security, Controls, Control objective and the methodology of IS Audit. These are discussed below.

IS RISKS AND RISK MANAGEMENT

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management involves identifying, measuring, and minimizing uncertain events affecting resources. Any Information system based on IT has its inherent risks. These risks cannot be eliminated but they can be mitigated by appropriate security. This security has to be implemented as per required control system envisaged by the management of the enterprise. IS

The author is member of the Institute. The views expressed herein are the personal views of the author and do not necessarily represent the views of the Institute.

Auditors are required to evaluate whether the available controls are adequate and appropriate to mitigate the risks. If controls are unavailable or inadequate or inappropriate, then there would be a control weakness, which has to be reported to auditee management with appropriate recommendations to mitigate them. Based on the point of impact of risks, controls are classified as Preventive, Detective and Corrective. Preventive controls prevent risks from actualizing. Detective controls detect the risks as they arise. Corrective controls facilitate correction.

INFORMATION SYSTEMS SECURITY

The risks in IT environment are mitigated by providing appropriate and adequate IS Security. IS security is defined as "procedures and practices to assure that computer facilities are available at all required times, that data is processed completely and efficiently and that access to data in computer systems is restricted to authorised people". The objective of information security is "the protection of the interests of those relying on information, and the information systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality, and integrity." For any organization, the security objective is met when:

- Information systems are available and usable when required (availability);
- Data and information are disclosed only to those who have a right to know it (confidentiality); and
- Data and information are protected against unauthorized modification (integrity). The relative priority and significance of availability, confidentiality, and integrity vary according to the data within the information system and the business context in which it is used.

Systems security encompasses the various layers of information systems such as the physical layer (physical aspects of IT) and logical layer (logical/software aspects). The physical layer would encompass physical and environmental security. The logical layer would encompass security at various layers such as Operating system, Network, Database and Applications Software. Security is as strong as its weakest link. Hence, it is critical to ensure that security that each of the layers is appropriately designed and implemented. Before implementation of security, it has to be designed building the information security model. This security model is based on overall management philosophy and guidelines. The overall nature of business, organisation structure, management philosophy and IT deployment would determine the type of security to be deployed in the enterprise.

IS Audit is expected to provide reasonable assurance to management on IT Governance encompassing the key information criteria of Quality (effectiveness, efficiency and economy), IS security (Confidentiality, Integrity and Availability) and Fiduciary (Compliance and Reliability). IS Auditors help their clients in understanding and managing the risks of IT thus enabling organizations to use leading edge technology and stay ahead in a competitive environment by implementing business and process-oriented controls. IS Audit involves primarily assessing the existence and adequacy of security.

CONTROLS AND CONTROL OBJECTIVES

Control refers to "The policies, procedures, practices and organizational structures that are designed to provide reasonable assurance those business objectives will be achieved and that undesired events will be prevented or detected and corrected". Controls are used to reduce or eliminate the causes of exposure to potential loss. Exposures are potential problems areas. All exposures have causes. Some categories of exposures are:

- Errors or omissions in data, procedure, processing, judgment, and comparison.
- Improper authorizations and improper accountability apply to procedures, processing, judgment, and comparison.
- Inefficient activity applies to procedures, processing and comparison.

Internal control refers to the system and the plan of an organisation and all the methods and procedures adopted by the management of an entity to assist in achieving managements' objective of ensuring, as far as practicable, the orderly and efficient conduct of its business, including adherence to management policies, the safeguarding of assets, prevention and detection of fraud and error, the accuracy and completeness of the accounting records, and the timely preparation of reliable financial information. Identifying control weaknesses forms core function of a IS Audit. This involves:

- Assessing conditions, their causes and effects.
- Gathering reliable evidence to support such assessments.

Control Objective is defined as: "A statement of the desired result or purpose to be achieved by implementing control procedures in particular computer operations". Identifying the control objectives and evaluating them is one of the primary tasks in IS Audit. The control objectives serve two main purposes:

- Outline the policies of the enterprise as laid down by the management: Provide understanding of how con-

trols are implemented in the enterprise.

- Used as a benchmark for evaluating whether control objectives are being achieved: During the process of audit, control objectives are used for evaluating whether controls are implemented and designed. They are reviewed for providing assurance on compliance with controls and providing recommendations.

Control objectives are obtained from the management and used for IS Audit or they could also be selected from relevant Audit and technology standards and adapted as per the needs of the assignment.

OVERVIEW OF IS AUDIT

IS Audit Process

The responsibility of assessing the risks and implementing appropriate security and controls is primarily that of the management. IS Auditors are expected to provide reasonable assurance to management whether information systems risks arising out of implementing IT have been adequately and appropriately addressed through relevant security and controls. IS Audit assignment primarily involves review of the IT risks so as to confirm whether adequate and appropriate controls have been implemented as designed by the management. The focus in IS Audit is on evaluating the IT controls and identifying areas of control weaknesses. In an IS Audit assignment depending on the type of audit, the auditor would be primarily interested in ensuring that:

- IT risks have been appropriately addressed;
- Required controls are available;
- Where available – assess whether they are adequate and appropriate;
- Identify the key areas of control weaknesses; and
- Recommend corrective steps for mitigating the risks.

IS AUDIT STEPS

IS Audit includes the following key steps:

1) Finalize scope of audit.
2) Identify related standards.
3) Perform specific tasks of IS Audit.
4) Execute audit as per audit phases.

1. FINALIZE SCOPE OF AUDIT

IS Audit refers to any audit that encompasses (wholly or partly) review and evaluation of automated information processing systems, related non-automated processes and the interfaces between them. This definition of IS Audit makes it clear that IS Audit could encompass all aspects of operations of the auditee or it may be focused on a particular area. IS Audit could be done by internal auditors or external auditors. It could involve review (view again) and evaluation (against a benchmark or set standard) of any or all aspects of IT processing in the enterprise including the interfaces. IS Audit encompasses any evaluation of IT processing in an enterprise regardless of the nature of the business operations or the technology deployed.

If IS Audit is done as part of compliance audit, the scope and objective would be determined by compliance requirement. However, as IS Audit is not mandatory, the need, scope, objective, frequency and area of coverage of such audit are primarily determined by the management. IS Audit may be conducted from any one or more of the following perspectives:

- Evaluation of IT Resources.
- Review of the Business Processes using Information Technology.

The most important task in performing any IS Audit assignment is to define the scope and objective of the assignment and area or coverage (terms of reference). Audit scope could be defined based on selection of the relevant IT processes or IT Resources or information criteria (security, quality or compliance) to be audited.

IS Auditors could be required to assist the management in identifying the scope, objective, area or criteria for the specific IS Audit based on materiality or criticality. The auditee management may also determine the exact scope, objective, area or criteria of IS Audit based on which the IS Audit can be executed. For example, many banks in India provide a detailed checklist with control objectives and information criteria based on which implementation audit is to be conducted at computerised branches.

2. IDENTIFY RELATED STANDARDS

Based on the scope and objective of audit, the related standards of Systems Audit are to be identified and adapted for use. The primary sources for these materials are:

- Auditing and Assurance Standards issued by ICAI\IFAC.
- IT Guidelines issued by IFAC.
- IS Audit Standards and Guidelines by professional bodies.
- Specific industry standards (for example, Banks, IT Companies)
- Technology standards as per technology deployed.
- Compliance requirements as relevant.

- Industry related controls
- Specific business related controls or guidelines.

Based on the relevant standards and audit requirements, IS Auditors should formulate control objectives which are in tune with the audit objectives. These control objectives should be used for conducting the audit and also ensure that they obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence

3. PERFORM SPECIFIC TASKS OF IS AUDIT

In the case of IS Audit, in addition to the audit tasks applicable to general audit, the following specific tasks need to be adapted and performed, as per the requirements of the assignment:

A. Study technical aspects

Gather evidential matter relating to technical aspects of systems under study, including all relevant documentation describing the computer facility, application programs, operating procedures, security procedures and so on. The focus is to begin from the peripheral controls (general controls) to application's controls.

B. Use unique techniques

IS Audit would require application of unique techniques to these efforts. For example, the audit-planning step includes review of technical documentation and interviewing technical specialists. The IS Auditor must understand the procedures for testing and evaluating Information Technology controls as relevant.

C. Audit Software usage

These procedures include the use of generalised audit software to survey and analyze the contents of data files or the use of specialised software to assess the contents of operating system parameter files and flow-charting techniques for documenting the automated applications.

D. Risk Analysis

Risk Analysis is an important technique used for identifying the area and extent of testing. The audit areas are assigned a one-digit priority number of 1, 2, or 3 based on their risk score. The highest risk areas receive the highest priority rating of 1, intermediate risk areas a 2, and lowest risk a 3, another category, known as "required" audits, is not analyzed because required audits are needed to satisfy government regulation, regulator policy, a senior management or audit committee request, or by the external auditor. The areas selected for IS Audit are to be based on a good risk model which considers such elements as internal controls, changes in procedure, transaction volume, previous audits, materiality of each area, and relevant external factors.

E. Evaluation of Internal Controls

There are different techniques for overall evaluation of internal controls. IS Auditors need to adapt the one which is most relevant for the audit. The ratings could be based on representation of controls into categories of good, fair, or poor controls or the ratings could be numerical, for example from 1 to 5. No.1 representing the best controls and No. 5 the worst controls. The higher the number, the poorer is the controls.

F. Using Standard audit programs and Internal Control Questionnaires (ICQ)

IS Audits would require audit programs to be prepared based on specific technology and business standards. These standard auditing programs and internal control questionnaires can be obtained from several sources. These audit programs and ICQs (also known as checklists) can be used as the main investigative tool, irrespective of the various activities in the audit area. The instructions and questions on these documents are to be executed and answered, and the answers are evaluated to identify weaknesses in the internal control system. An ICQ is used to collect information about transaction flow and the control system to help identify control points and locate non-existing controls. Standard ICQs are developed based on the standard controls that should exist in an area. Standard ICQs however, may not include coverage of special or unique activities.

4. EXECUTION OF AUDIT AS PER AUDIT PHASES

A typical IS Audit can be divided into seven phases comprising of different activities. Each succeeding phase builds upon the information found in previous phases and, therefore, increases the level of detail in the information collected and reviewed. Each of these phases is briefly discussed here.

I. Planning and scope summary
II. Preliminary review
III. Compliance testing
IV. Substantive testing
V. Reporting,
VI. Wrap up, and
VII. Follow-up.

I. PLANNING PHASE AND SCOPE SUMMARY PREPARATION

The planning phase includes the accumulation of information needed to define the auditing work to be performed. The hours needed to complete the work, the number of staff members and the mix of skills needed, and the start and completion dates for each phase are required by auditing standards. To comply with audit standards, the results of the planning phase must be documented, reviewed, and approved by all members of the audit team and audit management. This documentation can be accomplished by use of a standardized form known as "scope summary". The scope summary is a necessary, deliverable end product for every audit performed.

(i) Risks and Exposures

The IS Auditor must be aware of potential risk and exposures, their relationship with control objectives of the area, and the key controls, which serve to minimize or eliminate the risk and exposures. The IS Auditor must bear in mind, however, that for every risk and exposure, there is a cause, and the more specifically stated the risk and exposure, the closer the IS Auditor gets to defining the cause of the exposure.

(ii) Control Objectives

Controls are implemented to mitigate the risks. Controls always have a cost but they also have benefits. The cost could be in terms of time or money. Benefits could be in terms of reduction of risk or in terms of improving the effectiveness and efficiency of operations. Hence, lack of controls could result in a risk but their existence would cost the enterprise money. In any enterprise, it is crucial to balance the cost vs. benefits of controls. To do this, it is important that controls are not implemented for sake of controls but each of them serves a particular objective. The objective for the controls is termed as control objective. Control objectives define what is sought to be accomplished by implementing the control. They also specify the purpose for which control is being implemented. One of the most important steps in IS Audit is to identify the control objectives. The control objectives serve two main purposes:

- Outline the policies of the enterprise as laid down by the management.
- Used as a benchmark for evaluating whether control objectives are being achieved.

(iii.) Key Controls

Documented policies and procedures, segregation of duties, documented test standards, and supervisory review are examples of controls techniques, or key control procedures, that the area can use to effect the control objectives that minimize or eliminate risks. These items are documented in the scope summary to provide the audit staff with a reference tool during preliminary review and compliance testing. Evaluation of Internal control system would consider:

- Volume and nature of transactions.
- Nature, timing and extent of substantive procedures in various areas.
- Internal control systems get in-built into the applications.
- Inherent risks of Information Technology as deployed.

(iv.) Audit Objectives

"Objectives" refers to the ultimate purpose of the audit, in general or specific terms. The more generally stated the audit objectives are, the broader the audit scope. As the objectives become more specific, the audit programs required for review and testing zero in on increasingly particularized functions. Protecting application programs from unauthorized changes, ensuring that they are error-free, protecting data libraries from unauthorized access, and assuring complete data recovery in the event of destruction are example of various audit objectives. IS Audits tend to use specific audit objectives because such audits are targeted at specific environmental areas or applications systems.

II. PRELIMINARY REVIEW SCOPE SUMMARY

The objective of the preliminary review phase is to gain an overall understanding of the activities and functions within the audited area and the processing performed by the application. The end product (deliverable) consists of two factors, of which, one is the complete documentation of the flows for all transactions in the audited area or, in the case of a computer application, documentation of the elements of application processing, the second deliverable is the identification of existing controls and the identification of non existing controls.

III. COMPLIANCE TESTING (TEST OF CONTROLS)

The primary focus of compliance testing is to test whether controls as envisaged by management are in operation and working. Based on the results and reliance of the above tests, IS Auditor would determine the

extent of substantive testing to be conducted. Existing controls that appear adequate must be subject to compliance testing. The knowledge gained during the preliminary review will permit the IS Auditor to design proper procedures in order to test samples of source documents. These documents are examined so that the adequacy of control points for each of the transactions is verified. Compliance testing is used to verify the adequacy of internal control points documented in the relevant work papers. In developing the test procedures, the IS Auditor must consider the key controls and control objectives. The IS Auditor should design the test procedures to evaluate the key controls. The tests involve taking source documents, reports, and other company records and comparing them, in terms of timing and placement, with prescribed policies and procedures.

IV. SUBSTANTIVE TESTING: (TESTING OF DETAILED TRANSACTIONS)

In case the compliance testing reveals:

- There are insufficient application controls to ensure correct processing of data; or
- There are insufficient general controls to ensure basic integrity of system;

Then the IS Auditor would rely more on substantive testing approach, which involves detailed testing of transactions as required.

Substantive testing is that which validates the details of financial transactions and balance, whereas compliance-testing concentrates on validating the internal control procedures exercised over those financial transactions. Substantive testing validates the amounts of the transactions themselves. The key differences in the two types of testing are the objectives and the scope of the test. In case of compliance testing, the scope is controls themselves and objective is to test whether these have been implemented as envisaged by the management. In case of substantive testing, the scope is the sample of transactions or events identified for verification of integrity of processing and the objective is to test the integrity of transactions processed. The procedures and documentation for completing substantive test development, test execution, and documentation are the same as those used for compliance testing.

i. Identifying Control Weaknesses

Identifying control weaknesses involves assessing conditions and their causes and effects. Much time is spent obtaining reliable evidence to support such assessments. The IS Auditor must obtain sufficient evidence to support the assessment of the nature of the condition reported, its causes and its effect. These three elements are vital to adequate reporting of control weakness. In assessing the condition, the IS Auditor identifies what is wrong: in explaining its cause, the IS Auditor explains why the condition exists and in predicting its effect, the IS Auditor describes the detrimental effects (implications/consequence) that have occurred or can occur in the future if the problem is not corrected.

Although identifying condition cause and effect are vital elements of reporting control weaknesses, the most important element is the recommendation to management. This describes the fix, which is a cost-effective or enhancement to a procedure that will improve the functioning of the organization. Controls are used to reduce or eliminate these causes of exposure to potential loss. The IS Auditor evaluates the equality of the control, how effectively the control limits causes of loss (detection of preventive control) and how well it reduces loss after it occurs (corrective control).

V. REPORTING

The Audit report is the final result of audit. It must report the control weaknesses identified and suggest corrective remedial measures. Each of the finding must be ranked based on a risk ranking. Findings must be confirmed for correctness from the auditee management. IS Auditors should also get the feedback from user management on the recommendations.

The scope, objectives and format of Audit reports in case of compliance audits such as financial audit, balance sheet audit, tax audit, etc. are laid down by the regulations which also prescribe the formats of the report. However, in the case of IS Audit, as it is not mandatory, the format of the report could be defined by the auditee management or they can be adapted by the IS Auditor from the general reporting standards and formats. As in the case of compliance audit, IS Audit report is also a formal means for communicating the objectives of the audit, the auditing standards used (if required), the audit scope, the methodology used (if required), and the findings, conclusions and recommendations. The general standards and methodology adapted for reporting of compliance audit are to be followed. However, the format and content would be defined as per the deliverables of the assignment.

VI. WRAP UP

Wrap up is the final meeting held by the IS Auditor

with the senior management of the auditee. This would involve collection of all the documents, presentation of the finding and recommendations to the senior management and obtaining feedback on the audit. Follow up mechanism or procedures are also established. Wrap up meeting signifies closure of audit.

VII. FOLLOW UP

Follow up primarily refers to reviewing whether the recommendations provided to mitigate the control weakness identified have been rectified by the auditee. The first step in this process is to ensure that audit management responds to the audit report. Its response should include the actions it has taken, or plans to take, with respect to audit comments and recommendations. Management's planned action should include a timetable for implementation of any changes management response, once received, must be evaluated for its adequacy and the completeness and accuracy of its intention to comply. Executive management and advise them if the response is inadequate. These could be done by:

- Reviewing previous audit recommendations during the audit and reporting on any continuing control weaknesses or agreed recommendations not implemented.
- Obtaining agreed action plan from the auditee at the conclusion of the audit and forwarding it to the monitoring authority for implementation.

The methodology of follow up would be laid down by the auditee management as part of the audit responsibility. The IS Auditor has to accordingly follow it. Follow up is done to ensure successful implementation of the recommendations. This would also provide practical insights into problems on account of which recommendations may not have been implemented.

IS AUDIT IN BANKS

Sample of list of IS Audit Assignments with scope and objective as relevant to banks and its branches are briefly here:

The scope and objective of IS Audit assignment is defined by the bank's management. IS Audit assignment in banks could be broadly classified into two categories:

1. IS Audit at IT department (review of IT controls applicable across the bank).
2. IS Audit at computerised branches. The details of this audit would vary depending on the type of IT deployment at the branch.

An illustrative list of areas of IS Audits with their scope, objective and areas of review are briefly explained below. A IS Audit assignment at a bank or its branches covers one or more following areas:

1. Implementation Audit.
2. Environmental and physical access controls review.
3. Logical access controls review.
4. IS Operations review.
5. SDLC Controls review.
6. Business continuity planning review.
7. Application Controls and Data Security review.
8. IT security review.
9. IT Policies review.
10. Certification of Vendor software.
11. IT Training.

1. Implementation Audit

This audit covers review of controls over all the critical areas of IT operations in branch of a bank. The areas to be reviewed are provided by the bank with control objectives and checklists as relevant to the branch. This audit includes review of controls relating to environmental access, physical access, logical access, software installation, change management, parameter settings, business continuity, user management, etc.

2. Review of Environmental and Physical access controls review

This review covers the controls over the IT process of managing facilities specifically the environmental and physical security relating to Information Technology. This review is expected to provide assurance to the management that the process of Environment and physical access to IT resources are appropriately controlled and monitored so as to satisfy the business requirement of providing a suitable physical surrounding which protects the IT equipment and people against man-made and natural hazards. Environmental Access Controls are controls relating to facilities provided for housing IT resources such as the Controls relating to Physical location, Power sources – electricity, UPS, generator, AC, Fire extinguisher, smoke detector alarm, humidifiers, etc. Physical Access controls are controls relating to physical security such as Locks, security guard, door alarms, restricted entry, visitor control, video monitoring, etc.

3. Logical Access Controls review

This review covers the control over the IT process of ensuring systems security specifically related to logical access and is expected to provide assurance to the man-

agement that the processes in place in granting access to systems satisfies the business requirement of safeguarding information against unauthorised use, disclosure or modification, damage or loss. This review relates to the controls relating to the logical access to the data and information and its protection by providing access on a need to know on a need to do basis. This review covers access controls relating to Operating Software, Telecommunications Software, Database Software and Applications Software (access controls). The major focus areas of controls to be reviewed relate to Access controls at each layer of IT primarily from perspective of security. (Confidentiality, Integrity and Availability)

4. IS Operations controls review

This review covers the controls over the IT process of ensuring that there are appropriate controls relating to IS Administration, Organisation and Management such as formulation of policies, procedures and practices relating to Information Systems.

5. SDLC Controls review

This review covers the controls over the system development life cycle methodology adapted by the enterprise so as to provide an assurance that the business requirements are satisfied by the existing system and to be satisfied by the proposed new or modified system (software, data and infrastructure) are clearly defined before a development, implementation or modification project is approved. The system development life cycle methodology is reviewed to confirm whether the solution's functional and operational requirements are specified including performance, safety, reliability, compatibility, security and legislation.

6. Business Contingency Planning review

This review covers the Control over the IT process of ensuring continuous service and is expected to provide assurance that there are available processes that satisfies the business requirement so as to make sure IT services are available as required and to ensure a minimum business impact in the event of a major disruption. This review primarily deals with controls relating to the capability of the organization to meet any undesired events, which could disrupt the operations partially or wholly. The focus of this review is to assess the policies, procedures and practices in place to ensure that the organization is in a position to recover from any disaster affecting the IT and thus the operations.

7. Review of Application controls and Data Security review

This review covers the Control over the IT process of managing and protecting data and is expected to provide assurance that appropriate and adequate controls are available in the application software deployed at the enterprise and these satisfies the business requirement of ensuring that data remains complete, accurate and valid during its input, update and storage. This review involves review of controls available in the specified applications Package. This review involves assessment of controls at various stages such as Input, Processing, Output, Storage, Retrieval and Transmission. The available security features in the package relating to Confidentiality, Integrity and Availability of data are assessed. The prevailing Organization structure, policies, procedures and practices were mapped with the information systems to assess controls.

8. IT security review

This review involves evaluation of security in the IT environment at various layers. This involves assessment of security from the technology perspective. The review covers security at various layers of IT such as physical layer, network layer, OS Layer, database layer and applications.

9. IT Policies review

This review involves evaluation of policies, procedures and practices relating to the IT environment. This review involves assessment of policies to assess their adequacy and appropriateness as per the requirements of the enterprise.

10. Certification of Vendor software

This involves review of application software for assessing whether all the banking related controls as claimed by the vendor are met by the application. The primary objective of this assignment is to conduct Applications Review of the package so as to review and evaluate the availability, adequacy and appropriateness of controls from the banker's (user) perspective. The review is expected to provide reasonable assurance to the users on the availability, adequacy and appropriateness of minimum level of controls in the package, in general as per accepted standard and specifically as adapted to banking.

11. IS Audit Training

Banks require training programs for their IT and non-IT professionals. The areas of training could cover various aspects of IT implementation, IT Audit, Security and Control. ■