CONTENTS

1. Introduction on IS Audit

1.1 Introduction

‘The Working Group on Information Systems Security for the Banking and Financial Sector’ constituted by Reserve Bank of India enumerated that each Bank in the country should conduct ‘Information Systems Audit Policy’ of the Bank. Accordingly Information Systems Audit and Security cell prepare Information Systems Audit Policy. The fundamental principle is that risk and controls are continuously evaluated by the owners, where necessary, with the assistant of IS Audit function.

The business operations in the Banking and Financial sector have been increasingly dependent on the computerized information systems over the years. It has now become impossible to separate information Technology from the business of the banks. There is a need for focused attention of the issues of the corporate governance of the information systems in computerized environment and the security controls to safeguard information and information systems. The developments in Information Technology have a tremendous impact on auditing. Well-planned and structured audit is essential for risk management and monitoring and control Information systems in any organization.

1.2 Audit Objectives

Auditing is a systematic and independent examination of information systems environment to ascertain whether the objectives, set out to be achieved, have been met or not. Auditing is also described as a continuous search for compliance. The objective of the IS audit are to identify risks that an organization is exposed to in the computerized environment. IS audit evaluates the adequacy of the security controls and informs the management with suitable conclusions and recommendations. IS audit is an independent subset of the normal audit exercise. Information systems audit is an ongoing process of evaluating controls; suggest security measures for the purpose of safeguarding assets/resources, maintaining data integrity, improve system effectiveness and system efficiency for the purpose of attaining organization goals. Well-planned and structured audit is essential for risk management and monitoring and control of information systems in any organization.

1.2.1 Safeguarding IS assets

The Information systems assets of the organization must be protected by a system of internal controls. It includes protection of hardware, software, facilities, people, data, technology, system documentation and supplies. This is because hardware can be damaged maliciously, software and data files may be stolen, deleted or altered and supplies of negotiable forms can be used for unauthorized purposes. The IS auditor will be require to review the physical security over the facilities, the security over the systems software and the adequacy of the internal controls. The IT facilities must be protected against all hazards. The hazards can be accidental hazards or intentional hazards.

1.2.2 Maintenance of Data Integrity

Data integrity includes the safeguarding of the information against unauthorized addition, deletion, modification or alteration. The desired features of the data are described here under:

a. Accuracy: Data should be accurate. Inaccurate data may lead to wrong decisions and thereby hindering the business development process.
b. Confidentiality: Information should not lose its confidentiality. It should be protected from being read or copied by anyone who is not authorized to do so.
c. Completeness: Data should be complete
d. Reliability: Data should be reliable because all business decision are taken on the basis of the current database.
e. Efficiency: The ratio of the output to the input is known as efficiency. If output is more with the same or less actual input, system efficiency is achieved, or else system is inefficient. If computerization results in the degradation of efficiency, the effort for making the process automated stands defeated. IS auditors are responsible to examine how efficient the application in relation to the users and workload.

2. Audit in Computerized Environment

2.1. Understanding Computerized Environment

In this section we explain how a computerized environment changes the way business is initiated, managed and controlled.

Information technology helps in the mitigation and better control of business risks, and at the same time brings along technology risks. Computerized information systems have special characteristics, which require different types of controls. Technology risks are controlled by General IS controls and business risks are controlled using Application controls. Even though the controls are different, the objectives of the audit function do not change whether information is maintained in the computerized environment or a manual environment; the tools and techniques are different.

The changes in control and audit tools as well as techniques have resulted in new methods of audit. The internal controls are mapped onto the technology. These controls and their mapping need to be understood as also methods to evaluate and test these controls. The auditor must learn new skills to work effectively in a computerized environment. These new skills are categorized in three broad areas:

- First, understanding of computer concepts and system design;
- Second, understanding the functioning of Accounting Information System (AIS), an ability to identify new risks and understand how the internal controls are mapped on to the computers to manage technology and business risks.
- Third, knowledge of use of computers in audit.

Acquisition of these skills has also opened up new areas of practice for auditors like Information System Audit, Security Consultancy, Web Assurance, etc.

2.2. Accounting Information Systems in Computerized Environment

In this section we bring out the fact that Accounting Information System in the manual and computerized environment is not the same.

In the computerized environment accounting records are kept in computer files, which are of three types, namely master file, parameter file and transaction file. This classification is not based on the types of records but on the basis of need and frequency of updation and level of security required. File and record security is implemented using the facilities provided by the operating system, database and application software.

With the increasing use of information systems, transaction-processing systems play a vital role in supporting business operations. And many a times, a TPS is actually AIS. Every transaction processing system has three components—input, processing and output. Since Information Technology follows the GIGO principle, it is necessary that input to the system be accurate, complete and authorized. This is achieved by automating the input. A large number of devices are now available to automate the input process for a TPS. There are two types of TPS—Batch processing and On-line processing. The documents, control and security implementation is different for each system.

COBIT (Control Objectives for Information Technology) is an internal control framework established by ISACA for an information system. COBIT can be applied to the Accounting Information System. To apply the COBIT framework an organization should

- Define the information system architecture
- Frame security policies
- Conduct technology risk assessment
- Take steps to manage technology risks like
    - Designing appropriate audit trails; providing systems, software security; Having a business continuity plan; Managing IS resources like data, applications and facilities; Periodically assessing the adequacy of internal controls and obtaining independent assurance for the information system.

Thus, we explain the functioning of typical sales, purchase and pay roll accounting system in a computerized environment. In particular, we focus on the inputs required, application control, processing, reports generated, exception reports, files used and standing data used.

To enable an auditor to understand the accounting information system so that he can collect audit evidence, we have covered flowcharting techniques too.

2.3. Impact of IT on Economics of Auditing

In this section we have discussed the impact of IT on the nature and economics of auditing. With the emerging areas of practice and the auditors having acquired IT skills, the economics of auditing have also changed. During the past three decades, IFAC has issued several relevant standards for auditing in a computerized environment. These standards cover areas like risk assessment in a computerized environment, stand-alone computers, database systems, on-line information systems, etc. Some standards issued for the manual environment are also applicable here. AICPA and ISACA have issued standards covering various areas in IS audit. Some of its standards like standards on evidence, audit planning, etc. are relevant for financial auditors and find a mention in this section.

Information Technology also impacts audit documentation, reporting, work papers, etc. Auditing in a computerized environment integrates the skills and knowledge of traditional auditing, information systems, business and technology risks and IT impacts auditing, audit planning, audit risk, audit tools and techniques, etc. Since detection of risks can now be controlled using computer assisted tools and techniques, overall audit risks can be controlled and reduced.

This risk-based audit approach starts with the preliminary review. The next step is risk assessment. Under the audit approach, depending upon the intensity of the use of Information Technology, audit is done either through the computers or around the computers. Once the approach is decided, the next step is to assess general IS controls and application controls. Using CAATs, the controls are assessed, evidence is collected, evaluated and reports are prepared using the information systems.

2.4. Concept of Security

In this section we discuss the concept of security in detail. IS resources are vulnerable to various types of technology risks and are subject to financial, productivity and intangible losses. Resources like data actually represent the physical and financial assets of the organization. Security is a control structure established to maintain confidentiality, integrity and availability of data, application systems and other resources.

Few principles need to be followed for effective implementation of information security. These are: Accountability, which means clear apportionment of duties, responsibilities and accountability in the organization; Creation of security awareness in the organization; Cost-effective implementation of information security; Integrated efforts to implement security; Periodic assessment of security needs; and Timely implementation of security.

Information security is implemented using a combination of General IS controls and application controls. General IS controls include implementation of security policy, procedures and standards, implementation of security using systems software, business continuity plan and information systems audit.

Besides, various other types of controls are also used for implementation like: Framing and implementing security policy; environmental, physical, logical and administrative controls; Physical controls including locks and key, biometric controls and environmental controls; Logical controls like access controls implemented by the operating systems, database management systems and utility software are implemented through sign-on procedures, audit trail, etc; Administrative controls like separation of duties, security policy, procedures and standards; disaster recovery and business continuity plans; information systems audit, etc.

2.5. IS Management

Information systems audit is a process to collect and evaluate evidence to determine whether the information systems safeguard assets, maintain data integrity, achieve organizational goals effectively and consume resources efficiently.

The common element between any manual audit and IS audit is data integrity. All types of audits (information audits) have to evaluate the data integrity. Since IS audit involves efficiency and effectiveness, it includes some elements of management and proprietary audit too.

IS audit evaluates the IS management function. According to COBIT, there are five IS resources. People, application systems, technology, data and facilities. The IS management function can be divided into four phases, like any other management function.

- Management (which is equivalent for planning and organization)
- Implementation and deployment
- Directing and controls
- Audit and monitoring.

In this section, we discuss the most important activities and controls for each of the resources during each phase of information systems management. We also discuss what an IS auditor would like to review during each phase for each resource.
All said and done, it should never be forgotten that the heart of IS audit is the systems audit, which reviews the controls implemented on the system using systems software. Systems audit is a subject of skills acquisition and not knowledge acquisition. Included is a sample checklist for UNIX audit in the section.

2.6. Availability of Information Systems :

In this section we have discussed the availability of information systems. Security serves three purposes - confidentiality, availability and integrity. While access controls provide confidentiality and availability, business continuity process and back-up procedures provide availability.

Availability risk is one of the major technology risks. With an increase in the coupling of business processes with information systems, which are in turn exposed to technology risks, there is a dire need to have a disaster recovery plan in place. While insurance can provide compensation for the loss of resources, a disaster recovery plan puts various IS resources in place, if such disaster ever occurs. It is, therefore, a corrective control.

A business continuity plan begins with business impact analysis and involves risk evolution and loss estimates for the outage. On the basis of outage costs, disaster recovery resources are put in place. Owing to cost/benefit consideration, disaster recovery resources cannot be put in place for all types of disasters. These are put in place for the likely disasters and for critical applications. The estimations made and priorities set for the disaster recovery plans also give financial auditors an idea about the risks and importance of application. This can also be a factor while planning for audit in a computerized environment.

2.7. Access Control :

All information systems involve two basic software called the operating system and the database. Both have the ability to control access to the data and applications. The operating system controls access at the directory and file level, while the database controls access at the record and field level. In this section we discuss the capabilities of the operating systems to implement security.

Application controls are implemented using the access control facilities of operating systems and database systems. Both provide an interface between the application controls and general IS controls. To ensure data integrity, it is necessary to control access to the data, applications and other resources. All users must get just-minimum-access which has two aspects to it:

First only authorized users should have access.

Second even authorized users should not have full access. The access should be need based. For this, all operating systems have two types of facilities, namely, authentication and authorization. Authentication allows only the authorized users to access the systems. Authorization, allows just-minimum-access to the files and directory. To manage both these facilities in all operating systems there is a facility called systems administration. The first thing the auditors should do, when they start working under the new operating system is to get to know the authorization, authentication and system administration functions relating to these facilities. Fortunately, all operating systems have more or less the same type of facilities, so the learning becomes quicker.

2.8. Database Management :

Database provides two important features—data sharing and data independence. Data sharing means that the users and applications share data, and data independence means data is stored independent of applications. These features make the information system implementation easy and, at the same time, increase the security concerns. Database offers facilities like data dictionary and a database administrator to implement the database. A database management system also provides facilities to address the concerns raised by data sharing and data independence. Every database provides facilities to implement sign-on procedures (user identification and authentication) and authorization mechanisms. To maintain data integrity, the just-minimum-access rule should be followed. The database facilities are used to create the audit train and to implement application controls. The data files need to be backed-up regularly.

The IT Act has prescribed that all record retention rules are also applicable to electronic records. The Reserve Bank of India has also prescribed record retention rules for the banks and the IFAC has issued standards for database systems used in accounting information system. Oracle is the most-commonly used RDBMS in India and world over, providing facilities to implement access controls through sign-on procedures and authorization. Authorization is implemented through object ownership, granting of privileges, and creation of roles and assignment of roles to the users.

2.9. Application Controls and their Functioning:

In this section, we have explained various types of application controls and their functioning. Business faces two types of operational risks—business risks and technology risks. Technology risks are controlled and mitigated by general IS controls and business risks by application controls. However, it is difficult to draw a dividing line between the two since application controls are implemented on the facilities provided by general IS controls.

The primary purpose of application controls is data integrity. This is achieved by ensuring integrity of input, processing and output. Application control primarily deals with the audit objects. The objective of any audit is to verify the assertion made in the financial statements. Assessing the applications controls can assess all seven types of assertions, made in a financial statement. COBIT has dealt with application controls at length in all the phases of information systems management.

Application controls can be divided into:

Validation of input; Authorization of input; Completeness of input; Accuracy of input

Integrity of stored data; Integrity of standing data; Completeness and accuracy of standing data; Completeness and accuracy of processing; Restricted access to assets and data; Confidentiality and integrity of output.

Application controls being program procedures, there effectiveness can be tested either by continuous audit or by a substantive audit using general audit software. In the next section, we explain how general audit software can be used for assessing application controls.

2.10. Evaluation of Business Risks :

The job of a financial auditor is to evaluate business risks. Business risks are controlled

and managed by implementing application controls. Therefore, the primary duty of a financial auditor is to evaluate application controls to reduce the control risk to the minimum. Computers follow the garbage-in-garbage-out principle. It is, therefore, better if application controls are evaluated for compliance. Since application controls are program procedures, if they comply with the internal control policies of the company once, they shall continue to comply unless changed. However, as in the manual environment, compliance testing is difficult, indirect and requires higher cost, time and resources. Therefore, in most of the cases, substantive testing is done. Compliance testing is done only for the crucial systems.

The aim of substantive testing, or, for that matter, all types of testing is to evaluate the assertions made in the financial statement. That is, whether the financial statement depicts the true and fair picture. Since the auditor cannot do much to the inherent risks and control risks, he has to plan his audit to use such tools and techniques, as to reduce the detection risks. Computer assisted tools and techniques help here and more so general tool-set providing facilities to conduct substantive testing.

ACL is the market leader in the arena of general audit software. The software provides the facilities needed by an auditor to evaluate all the seven types of assertions made in any financial statement. In addition, it also offers the facility to create work papers crucial in any audit assignment, besides providing an option to understand the data and files.

ACL Software offers tools to understand the quantitative features of the data as well as the qualitative features of the data. Moreover, it provides facilities to conduct substantive testing.

To enable both, the analytical procedures and substantive testing at the transaction level, it has utility facilities like indexing, sorting, joining, setting relation, creating output files, exporting files, extracting files, etc.

ACL has an excellent feature to create the command log. This keeps a check on the auditor, improves the audit quality and also proves useful for work papers. Each ACL document, by default, has a log file. In addition, it can also be used for testing the controls implemented on the system like the security facilities of an operating system and database. Therefore, it can also help in systems audit.

2.11. Conversion Audit :

This section explains conversion audit. Conversion to the computerized environment is fast picking up in India. The process has also been accelerated by the enactment of the Information Technology Act, 2000 and the instructions from Chief Vigilance Commissioner to the banking sector to computerize 100% of their business. Data conversion is a part of any software project. It requires a lot of technical competence to be able to covert from one database to another and from one application to another. Conversion audit is conducted to check the accuracy of such conversion.

3. Audit Organization and Management

3.1 Organization Strategy

Chasing best practices is not enough to ensure a highly successful audit organization. To add value to the company and excel in the audit world, internal auditors must be agile in anticipating change, using resources, and partnering with management to address risks and improve operations.

The audit organisation or group which subscribes to just such a philosophy and has built what many of its peers have deemed a "world-class" organization over the last several years. The group has learned that to be successful it must generate an appropriate internal audit infrastructure, tailor audit approaches to each business unit within the company, and create "over-the-top" results by focusing on four basic elements: people, processes, electronic platforms, and focused collaboration with senior management.

3.1.1 Hiring the Right People

Internal auditing is organized regionally, with the chief audit executive located at the company's world headquarters, and audit groups located around the world.

The group is primarily focused on processes, including operations and business process and financial controls, throughout all areas of the company's businesses. A diverse group of auditors brings several skill sets to audit areas that include project management, manufacturing, supply management, and product marketing and sales.

The internal auditors who work for the group were hired both for their potential and their experience. Within the context of this framework, most of the auditors possess advanced degrees and are, at least, bilingual.

The audit group enhances the specific professional skills of newly hired experienced personnel by teaching them auditing techniques within the multifunctional electronic-systems platform. It is far more important for technical skills -- rather than audit skills -- to be the primary focus of this experienced group of people because deals with a wide range of technology products and services.

The attributes most important for less experienced auditors are a keen, analytical mind; a consultative outlook; and potential for future movement into a business unit. These characteristics should be coupled with a tremendous curiosity, a desire to learn, and a willingness to work hard in a fast-paced travel environment.

Once hired at , inexperienced internal auditors develop skills rapidly as they are exposed to a variety of business issues in several different companies. Typically, a team of two or three auditors will cover two or more major business processes during fieldwork that lasts up to three weeks. The auditors obtain a diversity of experience coupled with a commonality of basic operating and control principles that enable them to add more value to the business each day they are there. They are also given written performance evaluations during at least the first year to monitor progress and identify areas for improvement.

The overall goal within the group is to retain a small core of experienced auditors and to rotate the balance to operating units after they have been in the audit group for approximately three years. The constant mix and change of players within the audit organization results in immense personal satisfaction, diversity of work experience, and continual challenge.

3.1.2 **Improving Audit Processes**

Over the last several years, internal auditing worldwide has made significant changes to its audit processes. The techniques used hardly seem revolutionary, but have proven effective over time. Ten years ago, the audit environment was characterized by:

* Basic audit processes that had wasteful steps and redundancies.

* Minimal planning for individual audits.

* Fieldwork that lasted too long -- four to eight weeks -- and was often too detailed.

* Audit reports that took too long to issue.

* Hard-copy workpapers that were often weeks behind schedule and contained too much extraneous data.

* Disjointed audit follow-up.

* Key performance metrics that were not tracked.

* Audit customers who did not receive the auditors' full attention.

Beginning with the upgrading of personnel resources, the internal audit group began to take steps to improve its processes. These steps included:

* Mapping basic audit processes and making necessary changes to be more efficient and to add more value.

* Revamping guidelines for internal audit operations.

* Re-engineering the audit process to reduce cycle time, measure performance, and improve consistency.

* Introducing electronic audit platforms within Lotus Notes to gain significant efficiencies.

* Implementing a permanent quality process.

* Improving customer focus.

* Developing an audit mission and marketing brochure to help customers understand internal auditing's mission and the skills that the auditors bring to the table.

Metrics played a key role in the successful upgrading of audit group processes by measuring key processes for improvement. Other results of introducing metrics include:

* Audit planning has become more current and focused since auditors began requiring specific information in advance from audit customers.

* Fieldwork is more focused and is accomplished in two to three weeks.

* A draft audit report is now completed at the end of fieldwork.

* Final audit reports, complete with management action plans, are issued less than 30 days after fieldwork ends.

* Primary audit workpapers are electronic, streamlined, and completed within two weeks after fieldwork ends; secondary hard-copy workpapers are strictly limited and accessory only.

* Audit follow-ups include decision criteria by internal audit management to determine whether follow-ups will be in person or by letter and tracked electronically.

* Customer service has become a primary focus and includes a quality questionnaire completed by the customer after each audit.

* A full-time audit quality improvement process is in place to develop new and enhanced approaches to the audit function.

The quality improvement program has been an important aspect of internal auditing's overall process improvement initiative. The quality process has paid off in numerous improvements, including streamlined audit reports and a thorough audit follow-up process. Additionally, at the beginning of each year, the entire audit group brainstorms and prioritizes a list of internal audit projects aimed at improving audit processes. Each auditor selects one or more quality improvement projects for the year with the concurrence of the quality coordinator and general auditor. The auditors develop brief project descriptions and report on project status at quarterly quality meetings. These projects are completed outside of the normal audit assignments and monitored by an audit quality coordinator throughout the year. In the end, the projects result in tangible audit process improvements for the internal audit group.

During the improvement process, it became apparent that tying performance to compensation helps motivate auditors to undertake and deliver quality projects. For the auditors who will be rotating to other parts of the company, an Internal Auditor Quality Recognition Program, with achievement levels and corresponding substantial cash awards, has been developed. At the end of the year, a management committee, chaired by the audit quality coordinator, determines the program awards based on predetermined criteria. Award winners are then recognized at a group meeting. For the core staff that remains in the internal audit group, the quality improvement projects are a factor in determining merit compensation.

Another step in the overall internal audit quality improvement process involves holding in-person meetings with various companies external to to actively benchmark internal audit practices. The internal auditors share processes of interest with members of other organizations, who in turn brief the internal auditors on areas in which they have a particular focus. For example, the auditors saw different aspects of control self-assessment from meeting with other outside audit groups. From that, the internal auditors developed their own tool to fit -- a jointly facilitated self-assessment with a shared focus on operational improvements and controls within factories and projects.

Additional impetus was given to improving processes to meet the demands of the culture. For example:

* requires internal staff activities, including internal auditing, to bill for their services. The cycle time reductions in areas including fieldwork and reporting time were crucial in making the internal audit group competitive in this regard.

* Internal audit processes were made flexible and nimble to meet the challenges associated with constant change due to acquisitions and divestitures and business portfolio mix and emphasis.

* The processes needed to work, with modifications, for any situation. The internal auditors perform many nonstandard audits and special reviews based on management requests.

Robust and efficient processes are an integral part of building a world-class internal audit activity. However, many companies stop here, simply adopting best practices and benchmarking. The other elements -- people, electronic platforms, and focused collaboration -- are needed to work in concert with quality processes to produce the synergies and ultimately the results that mark leadership in internal auditing.

USING ELECTRONIC PLATFORMS

In the mid-1990s, decided to use Lotus Notes as its worldwide standard for groupware. Since then, internal audit has built a number of databases for audit processes using Lotus Notes. With this base, the internal audit group has developed and used the following tools, all accessible worldwide:

* ELECTRONIC WORKPAPERS

Incorporated into processes in late 1996, they've expanded over the years and are used in a different format by internal audit worldwide. These include separate sections within the workpapers for process flow documentation, interviews, key document descriptions, and even logistics information.

* BEST PRACTICES DATABASE

An important tool to cross-pollinate successful practices as auditors travel from location to location, it represents top processes of companies as identified by auditors.

* TIMEKEEPING

The database can be "sliced and diced" to analyze hours or days by job, audit activity, and auditor. It also can accumulate billing data as well as perform many other functions.

* E-MAIL
Includes electronic distribution of audit reports.

* REFERENCE DATABASE
Located within the group, the Internal Control Documents database includes past audit reports, audit follow-up analyses, audit report distribution lists, key document templates, presentations, minutes of information sharing staff meetings, and other reference information.

* AUDIT PRACTICES REFERENCE PROGRAMS
Compiled by area.

* AUDIT MANAGEMENT AND AUDIT PROGRESS DATABASES
Used for internal administration of audits -- audit numbers, location data, team members, status, audit follow-up, and more -- these databases are also available to company management as a status of planned and active audits.

* MANUFACTURING AND SUPPLY MANAGEMENT TOOL KITS
Repositories of data and techniques for these areas.

* INTERNAL GUIDELINES
Instructions for the operation of the audit group.

* COMPANYWIDE POLICIES AND PROCEDURES
Accounting and reporting guidelines for all of .

* CORPORATE DATABASES
Includes electronic expense reporting and news releases.
In addition, the auditors developed a kit of templates for key audit documents. The kit includes Word and Excel framework documents, such as audit

engagement letters, audit reports, management action plans replying to audit reports, auditor job performance evaluations, and the audit quality questionnaire sent to customers following an audit.

internal audit has also made extensive use of the Internet. The worldwide Web site has a tremendous volume of data, which includes everything from companies, products, and locations to employee benefit forms. Internal auditing designed its corner of the Web site to market and explain its activities and to present employment opportunities.

These electronic platforms have made a tremendous difference to auditors in terms of accessibility and ease of use of information, cycle-time reduction, and availability of reference material. These efficiencies have enabled the internal audit group to be more productive and to better serve its customers. Electronic platforms remove barriers of time, geography, and space limitations. Armed with skilled personnel, effective processes, and supportive electronic platforms, the auditors are ready to better partner with their customers.

3.1.3 Focusing on Collaboration

By listening and offering advice on business and control issues on a continuous basis, the senior internal audit team has created an effective network with senior management. The auditors add value by providing not only what clients are seeking but also what they may need, even if they are not aware of it. The auditors strive for a win-win environment by delivering a good mix of both.

performs a worldwide risk assessment on which it bases its audit plan. Continuous collaboration and one-on-one meetings enable the auditors to analyze risk on an on-going basis and expose hidden issues. These meetings, if they set the right win-win tone, can be frank expressions of needs by both parties to accomplish their respective tasks. Auditors recognize that the highest level of acceptance has been realized when customers call them for operational, control, and other corporate governance advice.

Generally during these meetings, a formal agenda -- beginning with recent key audits and future risks -- works best. The auditors work through these issues at a quickened pace, but when a nerve is hit, the auditors and management tackle it together. The auditors use various handouts -- such as portions of audit and risk analysis reports -- and other documentation to keep senior management focused on where they are headed in the larger environment. Management's comments and concerns are carefully noted and integrated into the audit plan frequently. The auditors' goals are to add value, to be timely, and, in times of trouble, to avoid the question: "Where were the auditors?" Being proactive with senior management helps prevent a "witch hunt" aimed at internal auditing when something goes wrong.

The auditors further the collaboration effort by following up on past audits, whether it be in-person, by e-mail, or by telephone. Internal auditors can prioritize new and potential acquisitions of companies, some of which may be small, for review.

By integrating people, audit processes, electronic platforms, and focused collaboration with senior management, audit groups can become world-class organizations. No one factor will do the task alone. The synergies of integrating these elements produce a compelling environment that fosters excellence. Any uccessful program must be ongoing and focused on continuous change. Seeking world-lass status is a never ending journey and not simply a destination along the way.

3.2 IS Audit as Review Management

The objectives of an information system audit are to obtain reasonable assurance that an organization safeguards it data processing assets, maintains data integrity and achieves system effectiveness and efficiency. In conducting an audit there are five major phases, planning the audit, test of controls, tests of transactions, tests of balances or overall results, and completion of the audit. This report looks at how the nature of the organization and its use of generalized application software affect the conduct of each of the phases.

The organization is a medium-size automotive servicing firm. The organization uses a local area network consisting of three microcomputers running software application packages. The microcomputers are placed in different locations for different functions. It runs application software packages that are well known, well tested, and supplied by a reputable vendor. All the applications are relatively straightforward.

Auditing must be properly planned to achieve the results that both auditors and the organization are looking for. In this first phase, planning the audit, the auditor needs to obtain an understanding of the accounting and internal control systems so as to plan the audit. The auditor should obtain an understanding of the complexity of the information system and also how the information system environment influences the assessment of inherent and control risks.

The auditor should start by conducting interviews with top management and information system personnel to gather information for the audit. The auditor must observe activities being carried out within the information system function, review working papers from prior audits and review information system documentation. The auditor needs to review the information collected so as to have a good understanding of all the controls that exist within the organization. Reviewing the information system control procedures will help to evaluate the risks to the integrity of accounting data presented in the financial reports.

The software used by the organization is well known, well tested, and supplied by a reputable vendor. The application software packages are already divided by the functions they perform, thus simplifying complexity issues for the audit. Given the fact that the application is well tested by the vendor, it can be implied that computer controls are in effect and should be very effective. Therefore, auditor needs to concentrate on the user controls that are in place to see how they can be improved. Two major control issues were raised in the case, that of modifications to the software and access to the central database. The general manager has given the assurance that no modifications were made to the software, and that no staff member has computer knowledge needed to carry out modifications to the software. This may be true but controls must be in place to ensure that no modifications are made without proper authority. Adequate controls must exist over the source code, object code and documentation of the package. It is mentioned that there is controlled access to the central database. The auditor must examine these controls since unauthorized access to databases can jeopardize the integrity of data.

Some other controls that the auditor should check are systems that allow secure issue of or choice of passwords, correct validation of password, secure storage of password and follow up on illicit use of passwords. There should be controls for unauthorized, inaccurate, incomplete, redundant, ineffective or inefficient inputs entered in the system. Input program should identify incorrect data entered and the program should use special code to correct data corrupted because of noise in a communication line. The local area network is very small, consisting of only three microcomputers but it still needs protection against natural threats and physical disasters thus it is necessary to protect the local area network.

If controls are in place and are well designed and applied the risk exist that the auditor will fail to detect actual or potential material losses or account misstatement at the end of the audit. Auditors must determine the audit risk. In deciding the level of inherent risk the auditor need to take into account that the organization is a medium-sized firm in an industry that is not subject to rapid changes. The industry is not subject to many treats and would not normally be a target for abuse. In this light it can be assumed that the inherent risk will be low. To determine the control risk the auditor should look at management and application controls. Management controls should be looked at first since if management controls are good there should be little need to go into in-depth application controls. If management enforces high quality documentation standards then it is unlikely that the auditor will have to review the documentation for each application. Given that the software is well known and well tested, the application controls should be strong. Therefore the control risk should also be very low for the organization.

At this point it can be concluded that the auditor should audit around the computer. The reasons for this are firstly the applications are relative straightforward and simple. Second, it is more cost effective to audit around the computer when a generalize application software is being used. The application software was provided by a reputable vendor and is well tested, and the application has not been modified according to the general manager. Thirdly, since the package is well tested a high reliance is placed on user controls rather than computer controls. Thus there is no need to go through testing of processing logic and control in an application that is already tested by the vendor. This would require technical expertise to duplicate a task performed by a reputable vendor.

In the second phase, test of controls, the auditor should go into more detail in reviewing the documentation of processes and analysis of the information the auditor is interested in. Controls should be analyzed for faultiness of defect. User and computer controls should be tested. Since the application is well tested, testing should focus on the reliability of user controls rather than the reliability of computer controls. Some of the controls that should be tested during this phase are; unauthorized, inaccurate, incomplete, redundant, ineffective or inefficient inputs entered in the program; output should be complete and accurate and distributed promptly to the correct recipient; secure issue or choice of passwords, correct validation of password, secure storage of password and follow up on illicit use of passwords; segregation of duties; availability of up-to-date backups, viable of up-to-date backups, whereabouts of backup storage units and usable restore system; reporting, recording and resolving incidents and operational failures; and continuity controls.

In the third phase, test of transactions, testing should be centered on checking to see if material loss or account misstatement has occurred or might occur due to erroneous or irregular processing of a transaction. The application software is straight forward with the necessary built in controls in place therefore there is no need to go through the entire system looking for transaction errors. The auditor should take a few transactions and trace them from beginning to ending process to verify weather transactions are handled effectively and efficiently.

In the fourth phase, testing of balances or overall results, the purpose is to gather sufficient evidence to make a final judgment on the size of the losses or account misstatements that might have occur or might occur when the information system function fail to safeguard assets, maintain data integrity, and achieve system effectiveness and efficiency. If auditors find that computer controls are weak or nonexistent they will need to do more substantive testing on detailed test of transactions and account balance.

However, in this case the vendor tested all computer controls and it is safe to assume that the controls are strong and this eliminates the need for the auditors to conduct more substantive testing. Selling of spare parts is a one of the major revenue earner for the organization. In this light this auditors should conduct a physical inventory of the spare parts to verify that the physical count and computer application count are the same. Other tests that can be done are to recalculate depreciation on fixed assets, and confirmation of receivables.

In the fifth phase, completion of the audit, additional test to bring the audit to a close are generally conducted. These include reviews for subsequent events and contingent liabilities. The auditor must then formulate an opinion as to weather material loss or account misstatements have occurred and issue a report. The auditor should provide management with a report documenting control weaknesses; identify potential consequences of these weaknesses and recommendations for remedial actions. It was notice that no controls are in place against unauthorized program changes, in that case auditors must note that weakness, letting management know that unauthorized changes can destroy the functionality of the application and suggest ways of elimination that treat.

Some recommendations the auditor can make are as follows; the need to strengthen security for the organizations information assets by developing disaster recovery plans and business continuity plans; reviewing of technical staff's access to programs and data; track of staff activities; limiting the files and other resources authenticated users can access and actions which they can execute; and development of internal controls to ensure against authorized program changes.

There is no right or wrong approach to conducting an information system audit. There are factors that must be taken into account during the planning phase of the audit; these factors determine the approach the auditor takes. As was seen in this case, the fact that it was a medium-size, low risk organization using a generalized application software that was not modified were the main factors that determined the approach that would be taken by the auditor.

4. Risk Based Audit Framework

4.1 Introduction to the Risk-Based Audit Framework:

This guide is intended to assist managers in meeting the *Policy on Transfer Payments* (PTP June 2000) risk-related requirements that support government-wide directions for more corporate and systematic management of risk in the design and delivery of programs. For example, emphasis is placed on incorporating risk in the initial stages of program planning by stipulating that:

- "The type of transfer payment that a department uses to meet its program objectives is determined by the departmental mandate, business lines, clients and **an assessment of risks."** The PTP also refers to the following two requirements that are fulfilled through the development of an RBAF:
- "It is government policy to manage transfer payments in a manner that is **sensitive to risks**, complexity, accountability for results and economical use of resources…" [Section 5.0];
- "Departments must develop a **risk-based audit framework** for the audit of contributions…" [Section 8.5]. A primary impetus for the government-wide management-change initiative on risk arose from observations and recommendations made in the *1997 Report of the Independent Panel on Modernization of Comptrollership in the Government of Canada*. The report found that:
- "…key responsibilities for governing bodies … [include]: understanding **the risks associated with the type, level and quality** of the service government decides to (or not to) provide, whether directly or indirectly, and **ensuring that appropriate means are in place to manage these risks**…"
- "…areas that increasingly demand managerial excellence …[include]: matching more creative and client-driven decision making and business approaches with **solid risk management**…" In this context, Treasury Board of Canada Secretariat (TBS) acknowledged the importance and benefits of systematic risk management as a strategic investment in the attainment of overall business objectives and demonstration of good governance. As a result, increased emphasis is being placed on working together, at all levels, to create

management regimes which are based on leadership and values, well-defined standards and control systems as well as **solid risk management**.

In addition to the PTP, TBS has promoted the integration of systematic risk management practices in other key policies and guidelines, such as:

- the *Integrated Risk Management Framework* (April 2001) which establishes the expectation that implementing the Framework will "strengthen accountability by demonstrating that **levels of risk are explicitly understood**"; and
- the *Active Monitoring Policy* (June 2001) which stipulates that "departments must actively monitor their management practices and controls **using a risk-based approach**." The sections which follow describe the underlying objectives and components of an RBAF and provide guidance in its development and preparation.

4.1.1 What is an RBAF?

The RBAF is a management document that explains how risk concepts are integrated into the strategies and approaches used for managing programs that are funded through transfer payments. The RBAF provides:

- background and profile information on the transfer payment program including the key inherent risk areas (internal and external) that the program faces;
- an explicit understanding of the specific risks that may influence the achievement of the transfer payment program objectives;
- a description of existing measures and proposed incremental strategies for managing specific risks; and
- an explanation of monitoring, recipient auditing, internal auditing, and reporting practices and procedures.

4.1.2 Why Do We Need an RBAF?

Transfer payment programs operate in an environment that involves many interconnections, including those that stem from global expectations, governance requirements, authorities and various risk drivers4. All these factors affect the design and implementation of the program. Risk-Based Audit Frameworks can cost-effectively and efficiently assist managers in operating in this complex environment by:

●enhancing managers' and employees' understanding and communication of risk and related mitigation options;

●strengthening accountability for achieving objectives and stewardship over public funds;

●facilitating managers' achievement of government-wide requirements for solid risk management; ●providing a basis upon which to create contingency plans;

●helping to secure funding for new or renewed programs; and

●enhancing information for decision-making.

4.1.3 Development and Implementation of the RBAF?

The key parties that should be involved in the development and implementation of an RBAF are as follows: ●Managers of the program who have primary responsibility for ensuring that the RBAF reflects an accurate and comprehensive analysis of potential risks to the achievement of objectives as well as cost-effective monitoring, mitigation and reporting strategies;

●Internal Audit and program staff who could provide expert advice and technical support in risk identification, assessment and monitoring as well as take a lead role in preparing the Internal Auditing section of the RBAF;

●Evaluation staff who could provide knowledge and expertise, in recognition of the potential for overlap between RMAFs and RBAFs and in cases where the RMAF and RBAF are being integrated; and

●TBS Program and Center of Excellence for Internal Audit analysts, who have assigned responsibilities and knowledge of program and RBAF requirements respectively, and can provide advice during their preparation. Delivery partners/co-deliverers and interested parties may also be involved as collaborators.

4.1.4 Planning and Preparing an RBAF

The level of detail included in an RBAF document will vary according to the nature, complexity and sensitivity of the programs. In planning and developing the level of information and effort required to prepare the RBAF, consideration should be given to the following:

●uncomplicated programs with low materiality and a straightforward accountability and risk management environment would require a less detailed and resource intensive RBAF;
●high priority and complex programs with significant materiality (relative to the overall departmental budget) and a diversified and complex environment would require a more detailed RBAF and a larger investment of time and effort;
●the breadth and complexity of the program's RMAF could be used as a guidepost for RBAF development; and
●meaningful information should be provided in each section of the RBAF. The next sections of this document will guide the reader through the components of an RBAF and the steps involved in their development.

4.2 Components of an RBAF

The RBAF consists of the following key components:

The preparation of the RBAF involves a systematic and analytical process. This section of the guide takes managers and specialist advisors through the distinct steps in this process – the product of each step being a key element of the final framework.

4.2.1 Introduction

●The RBAF should be introduced with a concise explanation of the purpose of the RBAF in context of PTP requirements and the demonstration of good governance.
●A brief description of the program background should be provided to set the overall context. Background information would include events giving rise to the program, the nature of the contribution agreement (i.e. payable, non-repayable), magnitude of the transfer payments and the timeframe of the funding authority. ●If program management chooses to integrate the RBAF with the RMAF, this section should be used to briefly outline the points and extent of integration.

4.2.2 Roles, Responsibilities and Relationships

a) Purpose This section should clearly delineate the respective roles and responsibilities of management and IA in fulfilling the PTP monitoring, auditing and RBAF requirements. A summary of the recipient's role and responsibilities for complying to terms and conditions should also be provided.

b) Process The PTP (Section 8.5) and the Guide on Grants, Contributions and Other Transfer Payments delineate the roles and responsibilities of management and IA.

- **Management** is responsible for ongoing financial and operational monitoring and the audit of recipient's compliance to terms and conditions and the audit of recipients. The audit of recipients can also examine whether results data is reliable.
- **Internal Audit's (IA)** role is to employ risk-based methodologies in planning and conducting audits to provide assurance on the adequacy of integrated risk management practices, management control frameworks and information used for decision-making and reporting on the achievement of overall objectives. Management is responsible for applying and describing the risk-based approach in the selection of recipient audits. If management is not familiar with a risk-based methodology, IA could be of assistance in discharging this responsibility. 10 While management has overall responsibility for the RBAF, IA is responsible for employing a risk-based approach in establishing whether the overall transfer payment program should be subject to audit. As such, IA should complete the Internal Auditing section [Section 6.0] of the RBAF. Managers and IA should consult as soon as the RBAF requirement had been identified. They should reach an agreement on the collaboration needed to complete the Recipient Auditing and Internal Auditing sections of the RBAF. To facilitate a common understanding of compliance and ongoing monitoring requirements, it may also be beneficial to articulate recipients' roles and responsibilities for meeting contribution agreement terms and conditions.

c) Product A statement of roles, responsibilities and relationships between PTP management, IA and recipients.

4.2.3 Program Profile

a) Purpose The Program Profile should provide the context and the key areas of inherent risk (Key Risk Areas) that evolve from the transfer payment program's objectives and environment. Overall, the profile assists the manager in:

- meeting good governance expectations through a sound understanding of the accountability and risk management environment; and
- conducting a more efficient and effective detailed identification and assessment of risk for the Risk Assessment and Management Summary in the next RBAF component.

b) Process The Program Profile should be developed with reference to the organization's outcomes and design information that has been compiled during recent business planning and the development of the RMAF. As a first step in the process, the "Performance Profile" and other pertinent RMAF data should be verified with participating managers. Clearly articulated objectives and context will provide the basis for further internal and external environmental analysis and identification of the Key Risk Areas that evolve from the mandate. In this context, for ongoing programs, any recent internal audit or evaluation should be described, particularly the effect that their results may have had on the program. In the case of a small, uncomplicated program, the Profile can be developed by the manager alone. However, as the complexity and magnitude of the program increases, greater detail will be required from key knowledgeable stakeholders to ensure all Key Risk Areas are identified and adequately described. Knowledgeable stakeholders include experienced program staff, internal audit and evaluation advisor(s) and, if deemed necessary, external stakeholders. The involvement of a risk management advisor may also be required, depending on the degree of program complexity.

c) Product The Profile should include:

- the background, underlying rationale, objectives and need for the program;
- the target population, resources, product groups, delivery mechanisms, TPP stacking provisions and governance structure; and
- the key internal and external areas of risk (Key Risk Areas) that evolve from the legislation, mandate, program design and/or operating environment where there is a potential for significant impact on performance (i.e. anticipates, in macro terms, the work to be done in the next section).

4.2.4 <u>Risk Identification, Assessment and Management Summary</u>

The key risks should ideally be identified, assessed, and associated mitigation measures either implemented or in progress, prior to the development of the proposed Treasury

Board submission (in the case of new policy initiatives, prior to the Memorandum to Cabinet). If available, the departmental Integrated Risk Management Framework (IRMF) would be a primary source of reference or at least a starting point.

a) **Purpose** The purpose of this component is to ensure an explicit understanding of the level of key risks. Through systematic risk identification, assessment and development of response or mitigation procedures, managers will acquire an explicit understanding of all aspects of key risks. Furthermore, this component provides insight into the main operational measures, including controls used to mitigate key risks and thereby contributes data relevant to the explanation of Program Monitoring presented in **Section 3.5**.

b) **Process** The preparation of the Risk Assessment and Management Summary section generally requires input from a team of managers and knowledgeable staff within the program area, supported by various functional groups.

The team should carry out the following steps: **Preparation Steps**

- Consider who should participate
- Clearly define risk
- Establish a time horizon
- Customize a risk matrix
- Consider other tool requirements

Process Steps

1. Understand Objectives

- Clearly articulate and understand the program's objectives with reference to the outcomes established in the RMAF Logic Model.

2. Risk Identification

- Identify risk areas (sources of risk) related to the achievement of objectives (e.g. events, hazards, issues, lost opportunities and circumstances that could lead to an impact on stewardship, delivery, outputs, outcomes, etc.); and
- Conduct a preliminary intuitive analysis of the risk level of each area (high, medium, low) to select the risk areas that require further analysis.

3. Risk Assessment

- Articulate the particular concerns and existing mitigation measures for the risk areas selected for detailed analysis; and
- Assess the likelihood and impact of an undesirable effect, given existing mitigation measures, to arrive at a residual level of risk.

4. Risk Response or Mitigation

●Establish incremental response strategies to avoid, share, transfer, accept and manage the risk.

5. Key Risk Summaries

●Summarize the Key Risks and related particular concerns, existing measures, and Incremental Risk Management Strategies.

c) Product The Risk Assessment and Management Summary should include:

●A methodology section which explains the risk definition and model;

●A brief description of the process steps followed;

●The identification of parties involved in the process;

●A Risk Matrix to explain the criteria and define the levels of impact and likelihood

●An elaboration of the Key Risk Areas that were used in the Profile section to explain the overall risk context of the program; and

●summaries of the Key Risks that were identified including particular concerns, existing mitigation measures and incremental risk response strategies, if required.

4.2.5 <u>Program Monitoring and Recipient Auditing</u>

a) **Purpose** The purpose of this section is to provide a description of the monitoring and recipient auditing practices, which are to be undertaken by management. It should reflect the risk identification and elaboration work done in the previous section; in particular, it should reflect the mitigation (in this case, monitoring or recipient auditing) of those risks for which the response was to implement controls. This section should reflect all activities related to monitoring of the overall program and the recipient's compliance with terms and conditions through detailed operational and financial procedures.

b) **Process Monitoring** The description of overall monitoring should demonstrate that management has those risks for which the mitigation strategy was controls covered by adequate means and measures. Typical monitoring objectives would include:

●Achievement of established outputs/outcomes;

●Risks or impediments to the achievement of outputs/outcomes;

●Due diligence in determining eligibility of recipients and the expenditures of funds;

- The efficient, effective and economical use of resources, and
- Whether or not the program is being administered in accordance with appropriate terms and conditions at all stages of the transfer payment life cycle (i.e. selection, administration, delivery and reporting).

The description of detailed monitoring of compliance should outline the operational and financial procedures, including:

- Interviews and documentation reviews to assess milestone achievements;
- Expense claim verification procedures;
- Stacking requirements verification procedures; and
- Reviews of recipient financial statements.

The existing and incremental mitigation measures for key risks, included in the Program Risk Assessment, Identification and Management Summary section, provide relevant and current information for the preparation of the overall monitoring section. The Results-based Management and Accountability Framework (RMAF) should also provide relevant information with regard to monitoring the achievement of outcomes.

Recipient Auditing Recipient auditing is often the only effective way to establish:

- That funds were used for intended purposes;
- Compliance with terms and conditions; and
- Reliability of results data.

Recipient Auditing is applicable to contribution agreements due to their conditional nature. In cases where contribution agreements allow recipients to establish sub-agreements, management may also choose to audit the third, fourth, etc. party recipient's sub-agreement activities; i.e. all the links of the chain through to the end recipient (and the original Terms and Conditions of the Contribution Agreement should provide for this). Particular attention should be paid to Alternative Service Delivery (ASD) arrangements, i.e. where another party delivers the funds to the end recipient on behalf of the program manager, as this arrangement is inherently higher risk than direct delivery to the recipient. Grant programs conduct strict eligibility checks before issuing grants. However, once grants are issued, there is no further requirement to verify the recipients' use of funds, i.e. recipient auditing is not applicable in this instance. The PTP sets out the requirement for a “risk-based” approach for determining whether or not an audit should be conducted and if conducted, its objectives, scope and extent. The risk methodology used here should be consistent with that used in the previous section for program risk identification, assessment and management. In fact, the results of the risk assessment performed in the previous section (particularly those risk factors having to do with the recipient) should be brought forward and augmented, as needed, by factors that may not have been identified there (e.g. knowledge of the recipient known by the Finance or Internal Audit groups, but not to the program manager) and further augmented by "audit risk" factors (i.e. risk factors having to do with the possibility of the auditor drawing the wrong conclusion – concluding that all is well when it is not or that all is not well when it, in fact, is).

This section should describe the process used for deciding on and planning recipient audits, considering the following steps:

1. Audit Objectives

●Establish the audit objectives to verify compliance with terms and conditions and, if required, the reliability of results data.

2. Risk Identification and Assessment Criteria

●Development of a risk-based matrix and criteria to analyse the level of risk associated with recipients of contributions.

3. Risk Factors Rating

●Consider each audit risk factor and assign a rating. Calculate the overall risk rating, as LOW, MEDIUM or HIGH risk.

4. Audit Planning Decisions

●Based on overall risk ratings, determine the nature, scope and timing and sampling strategy, if any, for conducting recipient audits (or, where the second, third, etc. party is acting on behalf of the program manager (i.e. an ASD arrangement), end party audits).

c) **Product** This section includes:

●a complete and concise explanation of existing and planned monitoring activities; and

●a summary of the methodology used and decisions taken on conduct of recipient audits, including cost.

4.2.6 <u>Internal Auditing</u>

a) Purpose An internal audit of a transfer payment program can provide valuable assistance to management by providing assurance as to the soundness of the risk management strategy and practices, the management control framework and practices and the information being used for decision making and reporting. Specifically, internal audits may examine whether:

●Due diligence is exercised with regard to the expenditure of public funds;

●The program is administered in accordance with the terms and conditions of the funding authority; ●Relevant legislation and policy (e.g. Sections 32, 33 and 34 of the Financial Administration Act and Transfer Payment Policy) are being respected;

●The program has a risk management strategy and whether systematic risk management is used, where the magnitude and complexity of issues would warrant; and

●The quality of information is adequate for decision-making.

b) Process The process for planning internal audits is risk-based and the responsibility of IA. Transfer payment program management should consult with IA as soon as the need for an RBAF is identified (preferably at the Memorandum to Cabinet stage or at least when the need for a submission has been identified) in order to make arrangements for IA input to the relevant RBAF components. To maintain consistency, the risk assessment methodology used for internal audit decisions should be the same as the one used for program and recipient audit risk assessment; i.e. the results of the program risk assessment should be brought forward and augmented by risk factors that the internal audit group may be aware of, but that the program managers were not (e.g. corporate support risk factors and “audit risk”). Refer to Appendix C for details. It is recognized that the internal audit function and related planning are ongoing and that, in the case of an ongoing program, they may have already considered the relative risk of the subject program and scheduled, or not, an audit of the program for a specific time in the future or an audit of the program may have already been performed recently. If that is the case, then it would suffice to indicate the results of the audit performed and/or the details of future plans, including expected costs. However, in the case of a new program a complete risk assessment would have to be retrofitted to the existing internal audit plan and the results described here, including objective, scope, timing and expected costs.

c) Product the products, which should be provided by IA, are:

- A description of the results of any recent internal audits performed;
- Anticipated audit objectives, scope timing and expected cost, in cases where the need for an audit has been affirmed by IA; and
- A description of the risk-based audit planning methodology used for all departmental programs (including Transfer Payment Programs);
- If it is decided that no internal auditing will be performed, there should be an explanation of that decision.

4. 2.7 Reporting Strategies

a) **Purpose** The final component of the RBAF ensures that plans are in place to systematically report (both internally and externally) on the results of ongoing monitoring, recipient auditing internal auditing and evaluation. (Note, if reporting of evaluation results is already provided for in the RMAF, it may simply be copied here for completeness purposes).

b) **Process** There are many potential users of this information and the reporting strategy should consider all of their needs (e.g. management decision-making, accountability and communication/information sharing). Potential users of risk information include program management, central agencies and internal and external stakeholders.

c) **Product** At the minimum, the reporting strategy should include a description of:

- Periodic reports which are produced for monitoring purposes;
- Agreed upon recipient audit reports;
- Evaluation reports;
- Internal audit reports that will be provided;
- Who is responsible (especially when multiple parties are involved) for producing reports; and ●The mechanisms (e.g. annual progress reports, mid-term reports, Departmental Performance Reports) and timeframes for reporting on operational monitoring, recipient and internal audits to the lead department, TBS, TB Ministers and/or Parliament.

4.3 RBAF/ RMAF Integration

Benefits of Integrated Performance and Risk Assessment and Reporting:

The PTP also requires that management develop a Results-Based Management and Accountability Framework (RMAF) to provide measurement and evaluation strategies for assessing the performance of a transfer payment program. The RBAF and RMAF are complimentary documents that provide managers with the means and measures for enhancing program monitoring and reporting. In this regard, the RBAF and RMAF have natural points of integration that relate to the typical analytical and planning approaches used by managers to monitor program operations and performance. For example, it is quite natural for program managers to simultaneously contemplate performance and risk issues when considering whether or not program objectives will be achieved. This integrated thinking facilitates the development of practices and procedures that fulfil the dual function of promoting the achievement of objectives and mitigating risks to performance. The links between performance and risk, including data collection elements (baseline data) and control frameworks, should be considered at the beginning of the program lifecycle. This integrated approach will assist in clearly identifying all objectives, the program context as well as potential internal and external risks to the achievement of objectives. In this regard, it is recognized that the RBAF must be “risk sensitive” and that the RMAF must be “performance sensitive”, i.e. linking risk to the program outcomes and performance measurement strategies.

5. IS Audit Standards

5.1 Code of Professional Ethics

The Information Systems Audit and Control Association, Inc. (ISACA) sets forth this *Code of Professional Ethics* to guide the professional and personal conduct of members of the Association and/or its certification holders.

Members and ISACA Certification holder's shall:

1. Support the implementation of, and encourage compliance with, appropriate standards, procedures and controls for information systems.
2. Perform their duties with due diligence and professional care, in accordance with professional standards and best practices.
3. Serve in the interest of stakeholders in a lawful and honest manner, while maintaining high standards of conduct and character, and not engage in acts discreditable to the profession.
4. Maintain the privacy and confidentiality of information obtained in the course of their duties unless legal authority requires disclosure. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities, which they can reasonably expect to complete with professional competence.
6. Inform appropriate parties of the results of work performed; revealing all significant facts known to them.
7. Support the professional education of stakeholders in enhancing their understanding of information systems security and control.

Failure to comply with this *Code of Professional Ethics* can result in an investigation into a member's or certification holder's conduct and, ultimately, in disciplinary measures.

5.2 IS Auditing Standards

The specialized nature of information systems (IS) auditing and the skills necessary to perform such audits require standards that apply specifically to IS auditing. One of the goals of the Information Systems Audit and Control Association (ISACA) is to advance globally applicable standards to meet its vision. The development and dissemination of the IS Auditing Standards are a cornerstone of the ISACA professional contribution to the audit community. The framework for the IS Auditing Standards provides multiple levels of guidance:

Standards define mandatory requirements for IS auditing and reporting. They inform:

– IS auditors of the minimum level of acceptable performance required to meet the professional responsibilities set out in the ISACA Code of Professional Ethics for IS auditors

– Management and other interested parties of the profession's expectations concerning the work of practitioners

– Holders of the Certified Information Systems Auditor (CISA) designation of requirements. Failure to comply with these standards may result in an investigation into the CISA holder's conduct by the ISACA Board of Directors or appropriate ISACA committee and, ultimately, in disciplinary action.

Guidelines provide guidance in applying IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure. The objective of the IS Auditing Guidelines is to provide further information on how to comply with the IS Auditing Standards.

Procedures provide examples of procedures an IS auditor might follow in an audit engagement. The procedure documents provide information on how to meet the standards when performing IS auditing work, but do not set requirements. The objective of the IS Auditing Procedures is to provide further information on how to comply with the IS Auditing Standards.

Resources should be used as a source of best practice guidance. The COBIT *Framework* states, "It is management's responsibility to safeguard all the assets of the enterprise. To discharge this responsibility as well as to achieve its expectations, management must establish an adequate system of internal control."

COBIT provides a detailed set of controls and control techniques for the information systems management environment. Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT information criteria.

As defined in the COBIT *Framework,* each of the following is organized by IT management process. COBIT is intended for use by business and IT management, as well as IS auditors; therefore, its usage enables the understanding of business objectives, communication of best practices and recommendations to be made around a commonly understood and well-respected standard reference. COBIT includes:

- Control Objectives—High-level and detailed generic statements of minimum good control
- Control Practices—Practical rationales and "how to implement" guidance for the control objectives
- Audit Guidelines—Guidance for each control area on how to obtain an understanding, evaluate each control, assess compliance and substantiate the risk of controls not being met
- Management Guidelines—Guidance on how to assess and improve IT process performance, using maturity models, metrics and critical success factors. It provides a management-oriented framework for continuous and proactive control self-assessment specifically focused on:
- – Performance measurement—How well is the IT function supporting business requirements? Management Guidelines can be used to support self-assessment workshops, and they also can be used to support the implementation by management of continuous monitoring and improvement procedures as part of an IT governance scheme.
- – IT control profiling—What IT processes are important? What are the critical success factors for control?
- – Awareness—What are the risks of not achieving the objectives?
- – Benchmarking—What do others do? How can results be measured and compared? Management Guidelines provides example metrics enabling assessment of IT performance in business terms. The key goal indicators identify and measure outcomes of IT processes, and the key performance indicators assess how well the processes are performing by measuring the enablers of the process. Maturity models and maturity attributes provide for capability assessments and benchmarking, helping management to measure control capability and to identify control gaps and strategies for improvement.

5.3 IS Auditing Guidelines

Selection of the most relevant material in COBIT applicable to the scope of the particular audit is based on the choice of specific COBIT IT processes and consideration of COBIT's information criteria.

In the case of this specific audit area, Review of Internet Banking, the processes in COBIT likely to be the most relevant are: selected

Plan and Organise IT processes, selected *Acquire and Implement* IT processes, selected *Deliver and Support, and selected Monitor*

and Evaluate. Therefore, COBIT guidance for the following processes should be considered relevant when performing the audit:

- PO1—Define a Strategic IT Plan
- PO3—Determine Technological Direction
- PO8—Ensure Compliance with External Requirements
- PO9—Assess Risk
- AI2—Acquire and maintain application software
- AI3—Acquire and maintain technology infrastructure
- AI4—Develop and maintain procedures
- AI5—Install and accredit systems
- AI6—Manage Changes
- DS1—Define and Manage Service Levels
- DS2—Manage Third-party Services
- DS3—Manage performance and capacity
- DS4—Ensure Continuous Service
- DS5—Ensure Systems Security
- DS8—Assist and Advise Customers
- DS10—Manage Problems and Incidents
- DS11—Manage Data
- M1—Monitoring the Process
- M2—Assess Internal Control Adequacy

The information criteria most relevant to an Internet Banking audit are:

- Primary: confidentiality, integrity, availability, compliance and reliability
- Secondary: effectiveness and efficiency

6. Use of Computer-Assisted Audit Techniques (CAATs)

6.1. Background

6.1.1 Linkage to COBIT Standards

6.1.1.1 Standard 060 (Performance of Audit Work) states "During the course of the audit, the IS auditor should obtain sufficient, reliable and relevant evidence to achieve the audit objectives. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

6.1.1.2 Standard 050 (Planning) states "The IS auditor should plan the information systems audit coverage to address the audit objectives and to comply with applicable laws and professional auditing standards."

6.1.1.3 Standard 030 (Professional Ethics and Standards) states "The IS auditor should exercise due professional care, including observance of applicable professional auditing standards."

6.1.2 Need for Guideline

6.1.2.1 Computer Assisted Audit Techniques (CAATs) are important tools for the IS auditor in performing audits.

6.1.2.2 CAATs include many types of tools and techniques, such as generalised audit software, utility software, test data, application software tracing and mapping, and audit expert systems.

6.1.2.3 CAATs may be used in performing various audit procedures including:

- Tests of details of transactions and balances
- Analytical review procedures
- Compliance tests of IS general controls
- Compliance tests of IS application controls
- Penetration testing

6.1.2.4 CAATs may produce a large proportion of the audit evidence developed on IS audits and, as a result, the IS auditor should carefully plan for and exhibit due professional care in the use of CAATs.

6.1.2.5 This Guideline provides guidance in applying IS auditing standards. The IS auditor should consider it in determining how to achieve implementation of the above Standards, use professional judgment in its application and be prepared to justify any departure.

6.1.2.6 This guidance should be applied in using CAATs regardless of whether the auditor concerned is an IS auditor .

<u>6.2. Planning</u>

6.2.1 Decision Factors for Using CAATs

6.2.1.1 When planning the audit, the IS auditor should consider an appropriate combination of manual techniques and CAATs. In determining whether to use CAATs, the factors to be considered include:

- Computer knowledge, expertise, and experience of the IS auditor
- Availability of suitable CAATs and IS facilities
- Efficiency and effectiveness of using CAATs over manual techniques
- Time constraints
- Integrity of the information system and IT environment
- Level of audit risk

6.2.2 CAATs Planning Steps

6.2.2.1 The major steps to be undertaken by the IS auditor in preparing for the application of the selected CAATs are:

- Set the audit objectives of the CAATs
- Determine the accessibility and availability of the organisation's IS facilities, programs/system and data
- Define the procedures to be undertaken (e.g., statistical sampling, recalculation, confirmation, etc.)
- Define output requirements
- Determine resource requirements, i.e., personnel, CAATs, processing environment (organisation's IS facilities or audit IS facilities)
- Obtain access to the organisation's IS facilities, programs/system, and data, including file definitions
- Document CAATs to be used, including objectives, high-level flowcharts, and run instructions

6.2.3 Arrangements with the Auditee

6.2.3.1 Data files, such as detailed transaction files, are often only retained for a short period of time; therefore, the IS auditor should make arrangements for the retention of the data covering the appropriate audit time frame.

6.2.3.2 Access to the organisation's IS facilities, programs/system, and data, should be arranged for well in advance of the needed time period in order to minimise the effect on the organisation's production environment.

6.2.3.3 The IS auditor should assess the effect that changes to the production programs/system may have on the use of the CAATs. In doing so, the IS auditor should consider the effect of these changes on the integrity and usefulness of the CAATs, as well as the integrity of the programs/system and data used by the IS auditor .

6.2.4 Testing the CAATs

6.2.4.1 The IS auditor should obtain reasonable assurance of the integrity, reliability, usefulness, and security of the CAATs through appropriate planning, design, testing, processing and review of documentation. This should be done before reliance is placed upon the CAATs. The nature, timing and extent of testing is dependent on the commercial availability and stability of the CAATs.

6.2.5 Security of Data and CAATs

6.2.5.1 Where CAATs are used to extract information for data analysis the IS auditor should verify the integrity of the information system and IT environment from which the data are extracted.

6.2.5.2 CAATs can be used to extract sensitive program/system information and production data that should be kept confidential. The IS auditor should safeguard the program/system information and production data with an appropriate level of confidentiality and security. In doing so, the IS auditor should consider the level of confidentiality and security required by the organisation owning the data and any relevant legislation.

6.2.5.3 The IS auditor should use and document the results of appropriate procedures to provide for the ongoing integrity, reliability, usefulness, and security of the CAATs. For example, this should include a review of program maintenance and program change controls over embedded audit software to determine that only authorised changes were made to the CAATs.

6.2.5.4 When the CAATs reside in an environment not under the control of the IS auditor, an appropriate level of control should be in effect to identify changes to the CAATs. When the CAATs are changed, the IS auditor should obtain assurance of their integrity, reliability, usefulness, and security through appropriate planning, design, testing, processing and review of documentation before reliance is placed on the CAATs.

6.3 Performance of Audit Work

6.3.1 Gathering Audit Evidence

6.3.1.1 The use of CAATs should be controlled by the IS auditor to provide reasonable assurance that the audit objectives and the detailed specifications of the CAATs have been met. The IS auditor should:

- Perform a reconciliation of control totals if appropriate
- Review output for reasonableness
- Perform a review of the logic, parameters or other characteristics of the CAATs
- Review the organisation's general IS controls which may contribute to the integrity of the CAATs (e.g., program change controls and access to system, program, and/or data files)

6.3.2 Generalised Audit Software

6.3.2.1 When using generalised audit software to access the production data, the IS auditor should take appropriate steps to protect the integrity of the organisation's data. With embedded audit software, the IS auditor should be involved in system design and the techniques will have to be developed and maintained within the organisation's application programs/systems.

6.3.3 Utility Software

6.3.3.1 When using utility software, the IS auditor should confirm that no unplanned interventions have taken place during processing and that the utility software has been obtained from the appropriate system library. The IS auditor should also take appropriate steps to protect the integrity of the organisation's system and files since these utilities can easily damage the system and its files.

6.3.4 Test Data

6.3.4.1 When using test data, the IS auditor should be aware that test data only point out the potential for erroneous processing; this technique does not evaluate actual production data. The IS auditor also should be aware that test data analysis can be extremely complex and time consuming, depending on the number of transactions processed, the number of programs tested, and the complexity of the programs/system. Before using test data the IS auditor should verify that the test data will not permanently affect the live system.

6.3.5 Application Software Tracing and Mapping

6.3.5.1 When using application software tracing and mapping, the IS auditor should confirm that the source code being evaluated generated the object program currently being used in production. The IS auditor should be aware that application software tracing and mapping only points out the potential for erroneous processing; it does not evaluate actual production data.

6.3.6 Audit Expert Systems

6.3.6.1 When using audit expert systems, the IS auditor should be thoroughly knowledgeable of the operations of the system to confirm that the decision paths followed are appropriate to the given audit environment/situation.

6.4. CAATs Documentation

6.4.1 Workpapers

6.4.1.1 The step-by-step CAATs process should be sufficiently documented to provide adequate audit evidence.

6.4.1.2 Specifically, the audit workpapers should contain sufficient documentation to describe the CAATs application, including the details set out in the following sections.

6.4.2 Planning

6.4.2.1 Documentation should include:

- CAATs objectives
- CAATs to be used
- Controls to be exercised
- Staffing and timing

6.4.3 Execution

6.4.3.1 Documentation should include:

- CAATs preparation and testing procedures and controls
- Details of the tests performed by the CAATs

- Details of inputs (e.g., data used, file layouts), processing (e.g., CAATs high-level flowcharts, logic) and outputs (e.g., log files, reports)
- Listing of relevant parameters or source code

6.4.4 Audit Evidence

6.4.4.1 Documentation should include:

- Output produced
- Description of the audit analysis work performed on the output
- Audit findings
- Audit conclusions
- Audit recommendations

6.5. Reporting

6.5.1 Description of CAATs

6.5.1.1 The objectives, scope and methodology section of the report should contain a clear description of the CAATs used. This description should not be overly detailed, but it should provide a good overview for the reader.

6.5.1.2 The description of the CAATs used should also be included in the body of the report, where the specific finding relating to the use of the CAATs is discussed.

6.5.1.3 If the description of the CAATs used is applicable to several findings, or is too detailed, it should be discussed briefly in the objectives, scope and methodology section of the report and the reader referred to an appendix with a more detailed description.