20th Meeting of INTOSAI Working Group on IT Audit

Country Paper of Supreme Audit Court of

Islamic Republic of Iran

By:

NABIOLLAH ELYASI

Principal Auditor

Sun City, South Africa

14-17 April 2011

DEVELOPING IT AUDIT PLAN

NABIOLLAH ELYASI[1]

INTRODUCTION

The use of Information and Communication Technology (ICT) within government entities has become increasingly significant in recent years, particularly Technology has increased the amount of data and information being processed and it has significantly impacted the control environment. ICT is also now a key component of government entities business strategies and core business processing activities.

Information Technology Auditing (IT auditing) began as Electronic Data Process (EDP) Auditing and developed largely as a result of the rise in technology in accounting systems, the need for IT control, and the impact of computers on the ability to perform services.

According to ASOSAI definition, IT audit may be defined as "the process of collecting and analyzing evidence in an IT environment in order to conclude against the pre-defined audit objectives".[2]

The pre-defined audit objectives would vary according to the nature of audit. If the audit were a financial audit, then the primary audit objective would be to render an independent opinion as to whether the financial statements of the audited entity reflect a true and fair view of the financial condition of the entity. Such an audit could also be termed as an IT audit if the entity's accounting system had been substantially computerized and so the auditor needs to form an opinion regarding the extent of reliance that can be placed on the IT system. On the other hand, if the audit is a VFM audit, then the primary audit object would be to assess whether the audited entity obtained value for money from its business operations. In this case too, the audit could be referred to as an IT audit if IT was being significantly used and so the auditor needed to form an opinion regarding the extent of reliance that could be placed on the IT system.

---

1 - General Auditor of Supreme Audit Court of I.R Iran , Email: nelyasi@gmail.com

2 - Introduction to IT Audit, Notes, ASOSAI, 2010

Another possible scenario is where audit assesses and reports on the IT system itself -the nature of a system**.** This has become quite common in view of the complexity and huge cost of information systems and the consequent need of the entity management for an independent assessment of the quality of the information system itself. In this case, the audit objective would generally be to determine whether the IT system safeguards assets, maintains data integrity, consumes resources efficiently and helps to meet organizational objectives.

IT Audit Process

IT audit process normally involves the following steps:

- Planning
- Evaluation of controls
- Evidence collection and evaluation
- Reporting and follow up

This process is depicted diagrammatically below.

Figure 1. A Typical Audit Cycle

Planning for IT Audit

One of the main responsibilities and more difficult tasks of the Chief IT Audit Executives (CIAEs) is to create the organization's audit plan. The objective of the audit plan is to determine where to focus the auditor's assurance and consulting work to provide management with objective information to manage the organization's risks and control environment.

Proper planning assists the auditor in:

- the direction and control of his work;
- highlighting critical areas ;
- allocation of scarce audit resources towards more important areas;
- setting time frame and targets for review work ;
- obtaining sufficient, reliable and relevant audit evidence and
- subsequently aid the auditee in sound decision making.

Strategic plan

This is long term planning, where the targets and objectives for the audit of IT systems of the auditees are determined by the SAI for a period spanning three to five years. This plan should cover all the auditee organizations and address issues like

- aims and long term objectives of audit;
- audit priorities and criteria for prioritization;
- how to re-orient audit techniques and methods to meet the changing requirements;
- human and infrastructure requirements and
- training needs .

Annual plan

This translates the long term plan into a program of work for the ensuing year. Planning here defines the aims and objectives of each of the major audits to be undertaken during the year, given the resources available within the SAI.

IT Audit Plan Process

Defining the annual audit plan should follow a systematic process to ensure all fundamental business aspects and IT-service support activities are understood and considered. Therefore, it is essential that the foundation for the plan be rooted in the organization's objectives, strategies, and business model. Figure 2 depicts a logical work-flow progression using a top-down approach to define the IT audit plan.

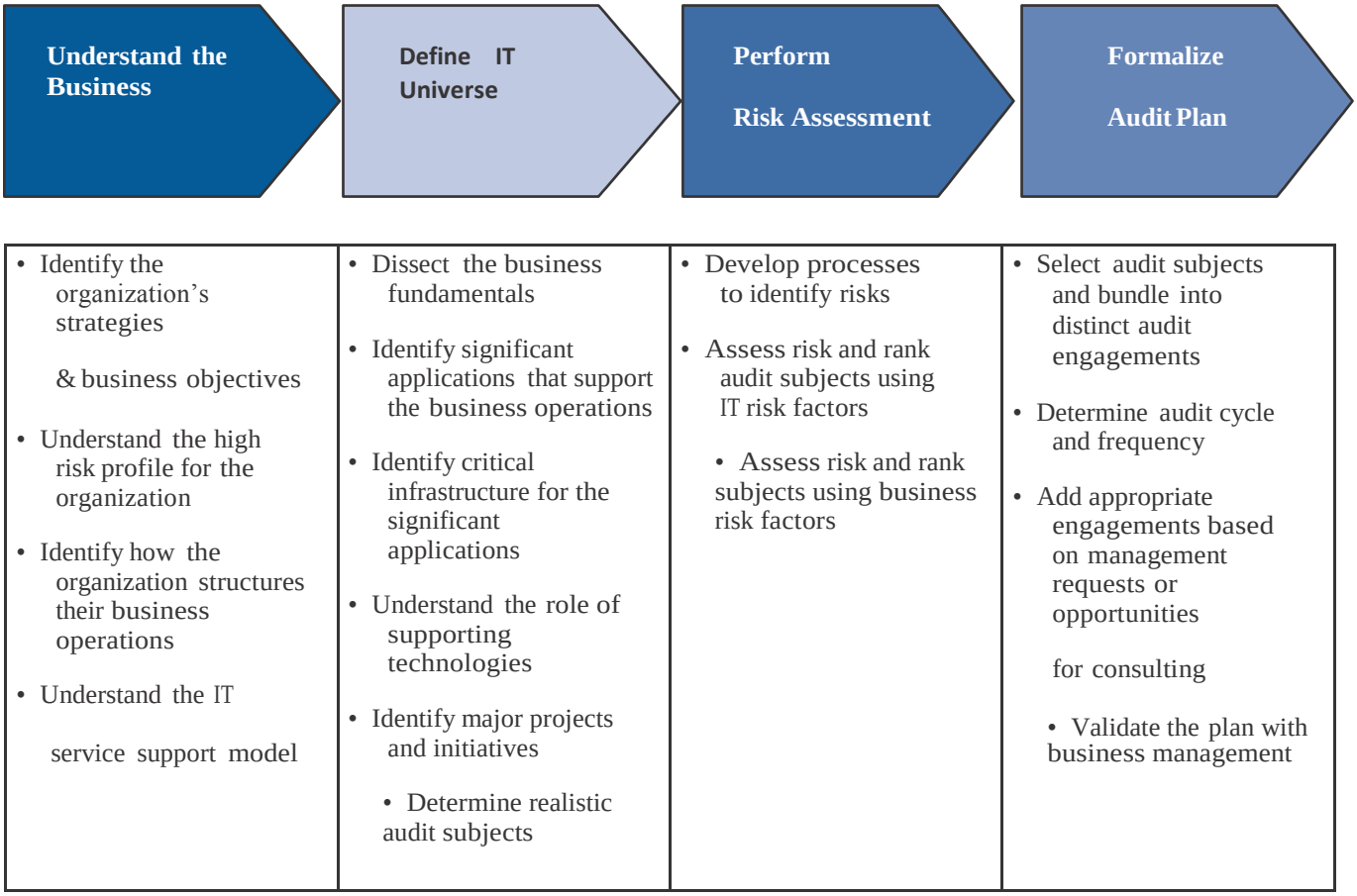

Figure 2. The IT audit plan process

1. Understanding the Business

The first step in defining the annual IT audit plan is to understand the business. As part of this step, auditors need to identify the strategies, company objectives, and business models that will

enable them to understand the organization's unique business risks. The audit team also must understand how existing business operations and IT service functions support the organization.

To become familiar with the organization, auditors first need to understand its objectives and how business processes are structured to achieve objectives (refer to figure 3). Auditors can use different internal resources to identify and understand the organization's goals and objectives, including:

- Mission, vision, and value statements.
- Strategic plans.
- Annual business plans.
- Management performance scorecards.
- Stockholder annual reports and supplements.
- Regulatory filings, such as those submitted to the Securities and Exchange Commission (SEC).

2. Defining the IT Audit Universe

The second step in defining the annual IT audit plan is to define the IT universe. This can be done through a top-down approach that identifies key business objectives and processes, significant applications that support the business processes, the infrastructure needed for the business applications, the organization's service support model for IT, and the role of common supporting technologies such as network devices. By using these technical components, along with an understanding of service support processes and system implementation projects, auditors will be able to create a comprehensive inventory of the IT environment.

Defining the IT audit universe requires in-depth knowledge of the organization's objectives, business model, and the IT service support model.

2.1 Examining the Business Model

Organizations can have different operational units and support functions to accomplish its objectives, which, in turn, have business processes that link activities to achieve their goals.

it is important for auditors to understand the company's IT environment when defining the IT universe and identifying the processes critical to the success of each unit.

Using a top-down approach to understand the organization's structure and activities can help auditors identify critical IT functionality processes that sustain the organization's operating units and support functions. However, variation in how similar business units perform their processes can add complexity to this analysis.

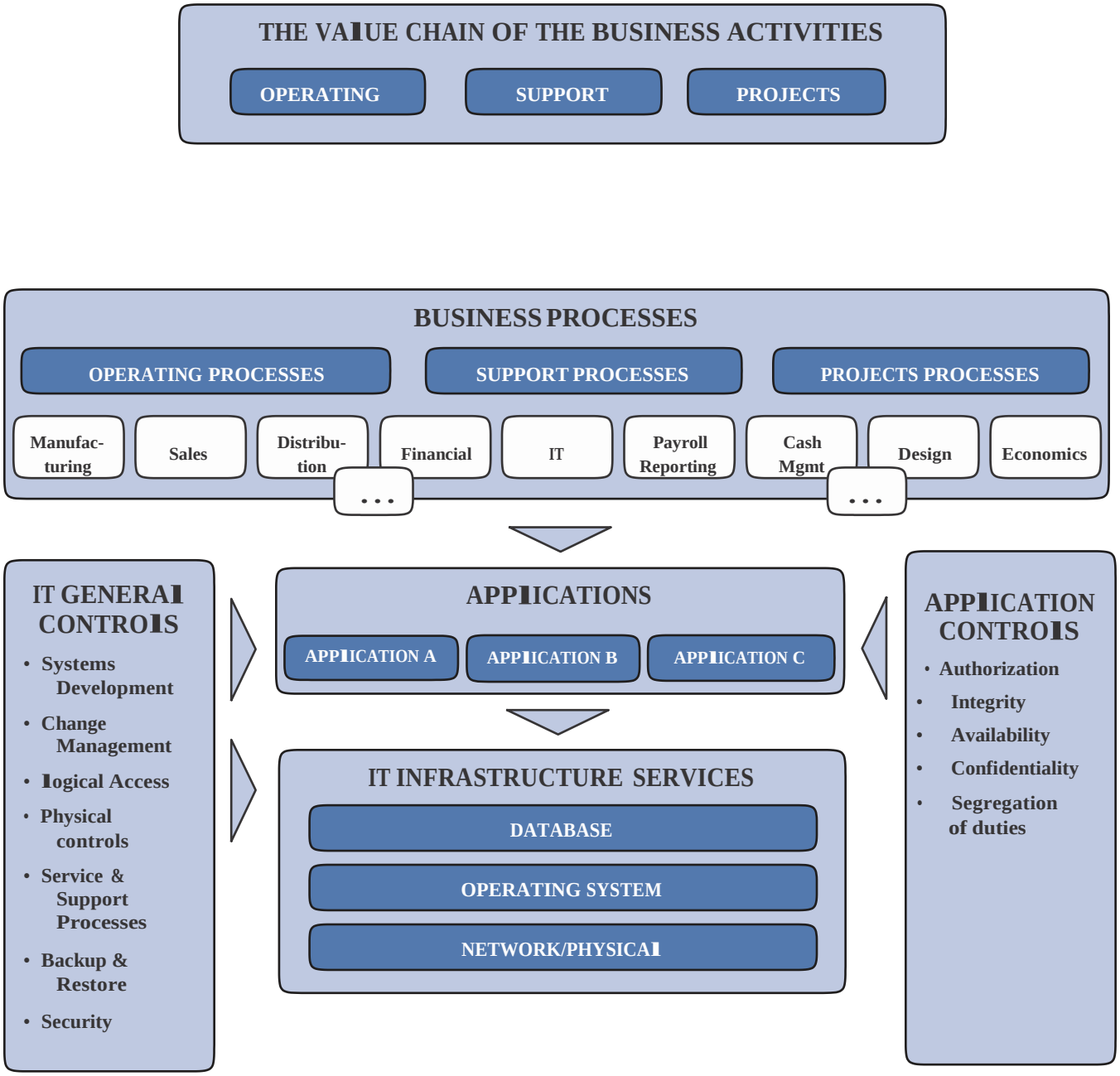

Figure 3. Understanding the IT environment in a business context[3]

[3] - Figure adapted and revised from: *IT Control Objectives for Sarbanes-Oxley*, 2nd Ed., used by permission of the IT Governance Institute (ITGI). ©2006 ITGI. All rights reserved.

2.2 Role of Supporting Technologies

Identifying supporting IT infrastructure technologies can be a simple process when detecting business activities that rely on key applications. However, it is much harder to associate the use of supporting technologies, such as the company's network, e-mail application, and encryption software, to business objectives and risk.

2.3 *Centralized and Decentralized IT Functions*

Auditors need to identify centrally managed IT functions that support the entire or a large portion of the organization. Centralized functions are good candidates for individual audits in the IT audit universe and include network design and security administration, server administration, database management, service or help desk activities, and mainframe operations.

A similar approach can be taken for decentralized IT functions, where each physical location might represent a separate audit subject. Depending on the location's size, the site's audit may review general and technical controls for each infrastructure stack layer.

2.4 IT Support Processes

Even if the organization has a decentralized IT function, it may have standardized support processes. Organizations that are striving to be high-performing organizations understand the importance of having standardized support processes across their operating units regardless of the business model. Examples of standardized support processes include service desk activities as well as change, configuration, release, incident, and problem management procedures.

2.5 Business Applications

CIAEs need to determine which audit group will be responsible for the planning and oversight of business application audits. Depending on how the audit function operates, business applications can be included as part of the IT audit universe, business audit universe, or both. There is a growing consensus among audit functions that business applications should be audited with the business processes they support. This provides assurance over the entire suite of controls — automated and manual — for the processes under review, helps to minimize gaps and overlaps of audit efforts, and minimizes confusion over what was included in the scope of the engagement.

3. Performing a Risk Assessment

After the IT universe is defined, a systematic and uniform assessment of risk across all subjects should be the next step in determining the annual audit plan.

The IIA defines *risk* as "the possibility that an event will occur that could affect the achievement of objectives, which is measured in terms of impact and likelihood."[4] Therefore, it is vitally important for organizations to determine the contents of their risk portfolio periodically and perform activities to manage risks to an acceptable level.

The risk assessment needs to examine the infrastructure, applications, and computer operations or components that pose the greatest threat to the organization's ability to ensure system and data availability, reliability, integrity, and confidentiality.

In addition, auditors need to identify the effectiveness and usefulness of risk assessment results, which should be directly predicated on the methodology employed and its proper execution.

Performing the risk assessment correctly is paramount to ensuring relevant IT risks *are* identified and evaluated effectively and adequate mitigation measures take place.

According to Institute of Internal Auditors' (IIA's) Practice Advisory 2110-1: Assessing the Adequacy of Risk Management Processes, risk management processes should have five key objectives:

• Risks arising from business strategies and activities need to be identified and prioritized.

• Management and the board need to determine the level of risk acceptable to the organization, including the acceptance of risks designed to accomplish the organization's strategic plans.

• Risk mitigation activities need to be designed and implemented to reduce or otherwise manage risk at levels that are acceptable to management and the board.

• Ongoing monitoring activities need to be conducted to reassess risk periodically and the effectiveness of controls to manage risk.

• The board and management need to receive periodic risk management process reports. The organization's corporate governance processes also should provide periodic communication of risks, risk strategies, and controls to stakeholders.

---

[4] - *International Standards for the Professional Practice of Internal Auditing*, p. 17.

According to The Research Foundation's *Assessing Risk*, there are three approaches to measuring risk and impact[5]:

1. **Direct probability estimates and expected loss functions or the application of probabilities to asset values to determine exposure for loss.** This process is the oldest and not considered a best practice.

2. **Risk factors or the use of observable or measurable factors to measure a specific risk or class of risks.** This process is favored for macro-risk assessments, but is not efficient or particularly effective for micro-risk assessments, except when auditable units are homogeneous throughout the audit universe as in branch, location, or plant audits.

3. **Weighted or sorted matrices or the use of threats versus component matrices to evaluate consequences and controls.** This method is superior for most micro-risk assessments.

According to *Assessing Risk*, three types of risk factors are commonly in use — subjective risk factors, objective or historical risk factors, and calculated risk factors.

1. **Subjective risk factors.** Measuring risk and its impact requires a combination of expertise, skills, imagination, and creativity.

2. **Objective or historical risk factors.** Measuring risk factor trends can be useful in organizations with stable operations

3. **Calculated risk factors.** A subset of objective risk factor data is the class of factors calculated from historical or objective information. These are often the weakest of all factors to use because they are derivative factors of risk that is further upstream.

Due to these risk factors, CIAEs and IT auditors must design and use a risk impact model that fits their organization.

3.1 IT Environment Factors

Different factors and analysis techniques should be considered to understand the operational environment and its unique risks. This is because an organization's control environment complexity will have a direct effect on its overall risk profile and system of internal control. Important factors to consider include:

- The degree of system and geographic centralization (i.e., distribution of IT resources).
- The technologies deployed.

[5]- The IIA Research Foundation's *Assessing Risk, 2nd Edition*, 2004

- The degree of customization.
- The degree of formalized company policies and standard (i.e., IT governance).
- The degree of regulation and compliance.
- The degree and method of outsourcing.
- The degree of operational standardization.
- The level of reliance on technology

3.2 *Steps in Risk Analysis*

The steps that can be followed for a risk-based approach to making an audit plan are:

- Inventory the information systems in use in the organization and categorise them.
- Determine which of the systems impact critical functions or assets, such as money, materials, customers, decision making, and how close to real time they operate.
- Assess what risks affect these systems and the severity of impact on the business.
- Based on the above assessment decide the audit priority, resources, schedule and frequency.

4. Formalizing the IT Audit Plan

Defining the IT audit universe and performing a risk assessment are precursor steps to selecting what to include in the IT audit plan. While everything in the IT audit universe could be reviewed on a recurring basis if the availability of resources is unlimited, this is not the reality for most internal audit functions. Consequently, CIAEs must create an IT audit plan within the constraints of the audit function's operating budget and available resources.

*4.*1 The Dynamic Nature of the IT Audit Plan

As technology continues to change, so does the arrival of new and potential risks, vulnerabilities, and threats to the company. In addition, technological changes may prompt a new set of IT goals and objectives, which in turn leads to the creation of new IT initiatives, acquisitions, or changes to meet the organization's needs.

An important point to consider when drafting the audit plan, therefore, is the organization's dynamic nature and its ongoing changes.

More specifically, auditors need to consider the higher rate of IT change compared to changes in non-IT activities, the appropriate timing of a system's SDLC phases, and the results of SDLC audits. In addition, auditors need to consider the specific source of the change.

4.2 Audit Plan Principles

IT auditors should consider the following advisory for the IT Audit Plan:

1. Planning should be involve establishing goals, schedules, staffing, budgeting, and reporting.
2. IT audit activities should be capable of accomplishing the goals within a specific time and budget and be measured in terms of, at least, targeted dates and levels of accomplishment.
3. The plan should include the work schedule with activities to be performed and their key planned dates, as well as estimated efforts in terms of their timeframe for completion and resources.
4. The plan should be prioritized based on:

a. Dates and results of the last audit engagement.

b. Updated assessments of risks and effectiveness of risk management and control processes.

c. Requests by the board and senior management.

d. Current issues relating to organizational governance.

e. Major changes in the business, operations, programs, systems, and controls.

f. Opportunities to achieve operating benefits.

g. Changes to and capabilities of the audit staff. (Work schedules should be sufficiently flexible to cover unanticipated demands on the internal audit activity.)

4.5 The IT Audit Plan Content

The content of the IT audit plan should be a direct reflection of the risk assessment described in previous sections.

The plan also should have different types of IT audits, for example:

• Integrated business process audits.

• Audits of IT processes (e.g., IT governance and strategy audits, as well as audits of the organization's project management efforts, software development activities, policies and procedures, COBIT/ISO/ITIL processes, and information security, incident management, change management, patch management, and help desk activities).

• Business projects and IT initiative audits, including software development life cycle (SDLC) reviews.

• Application control reviews.

• Technical infrastructure audits (e.g., demand management reviews, performance reviews, database assessments, operating systems audits, and operation analyses).

• Network reviews (e.g., network architecture reviews, penetration testing, vulnerabilities assessments, and performance reviews). To verify each audit provides appropriate coverage, auditors can incorporate the following elements as part of the audit:

• IT general controls, application controls, and infrastructure controls.

• Contributions to operational reviews, financial reviews, and compliance reviews.

• Main control objectives (i.e., segregation of duties, concentration of duties, and security, among others).

• New IT trends and their threats, innovations, and impact.

• All IT layers of the stack.

Conclusion

IT Audit can generally be described as "the process of obtaining and evaluating evidence to determine whether an IT system safeguards the organizational assets, uses resources efficiently, maintains data security and integrity and fulfils the business objectives effectively."[6]

As The Institute of Internal Auditors' (IIA's) Standard 2010, the Chief IT Audit Executives (CIAEs) should establish risk-based plans on at least an annual basis to determine the priorities of the internal audit activity, which, in turn, should be consistent with the organization's goals and strategies.

The objective of the audit plan is to determine where to focus the auditor's assurance and consulting work to provide management with objective information to manage the organization's risks and control environment.

Formalizing the audit plan is the final step of the information and analysis gained by understanding the organization, inventorying the IT environment, and assessing risks .

As the availability of resources is not unlimited, CIAEs must create an IT audit plan within the constraints of the audit function's operating budget and available resources.

[6] - Introduction to IT Audit, Student Notes, INTOSAI IT AUDIT COMMITTEE , 2007

References

1- Introduction to IT Audit, Student Notes, INTOSAI IT AUDIT COMMITTEE, 2007.

2- Introduction to IT Audit, Notes, ASOSAI, 2010.

3- IT Audit Guidelines, 6th ASOSAI Research Project, ASOSAI, September 2003

4- Kirk Rehage and et all, Developing the IT Audit Plan, Copyright by The Institute of Internal Auditors, 2008.

5- Elyasi Nabioolah, IT AUDIT workshops pp, 2010.