TRIBUNAL DE CONTAS DA UNIÃO

GET.IT

Governance Evaluation Techiniques for Information Technology

Msc. Marcio Rodrigo Braz, CISA and Diego Hulse
Department of External Control of IT (SEFTI)


Welcome to Brasília!!

Let’s get started!

So, why did we get involved into this project?

TCU has been conducting broad IT Governance evaluation of brazilian federal organizations since 2007.

This means 372 entities of the three branches (executive, legislative, judiciary)

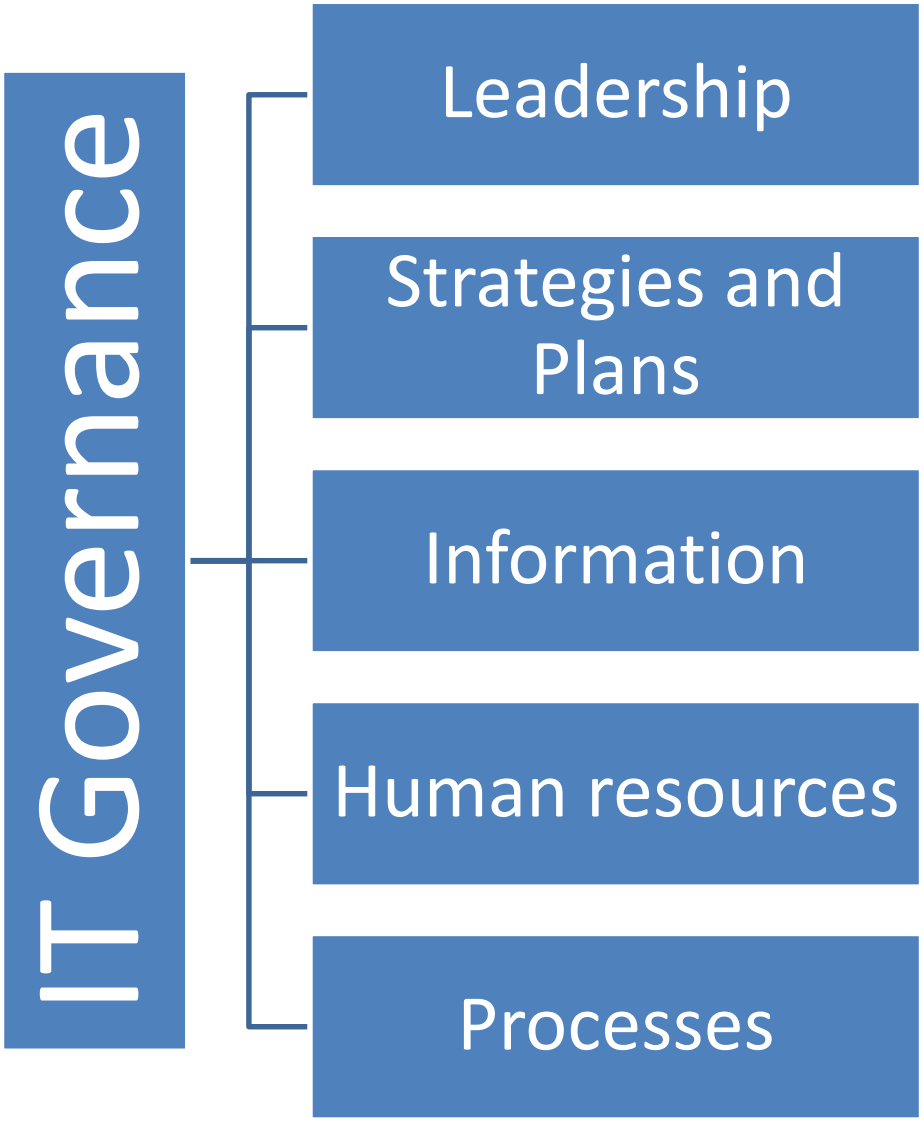
This is how it works...

Survey – Year 1

Year 2 – audits in order to check answers and the implemented processes

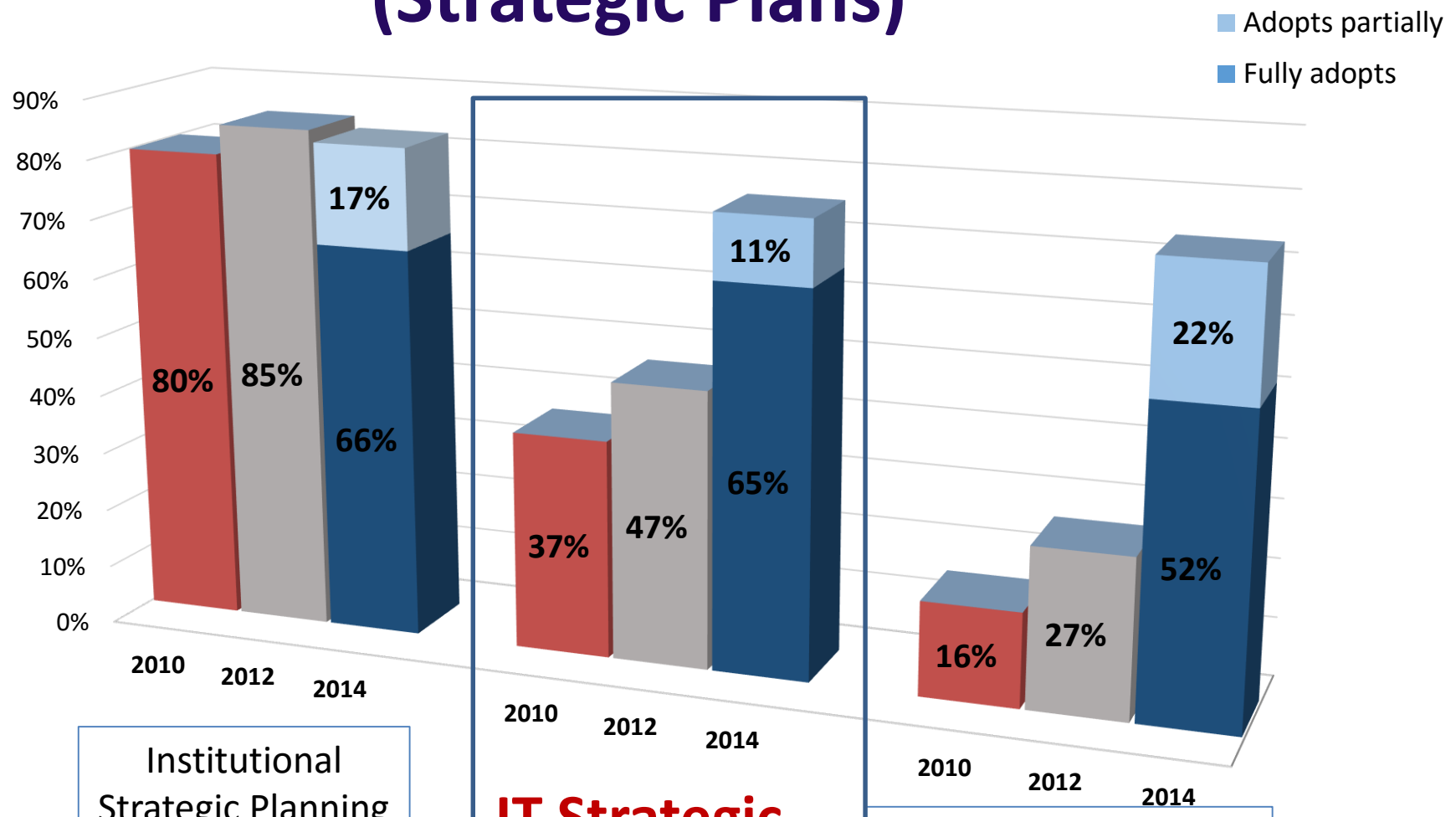
It covers a lot...

more than 200 itens



After some time, in some areas we may already see improvement...

Information Provided (Strategic Plans)



Institutional Strategic Planning

IT Strategic Plan

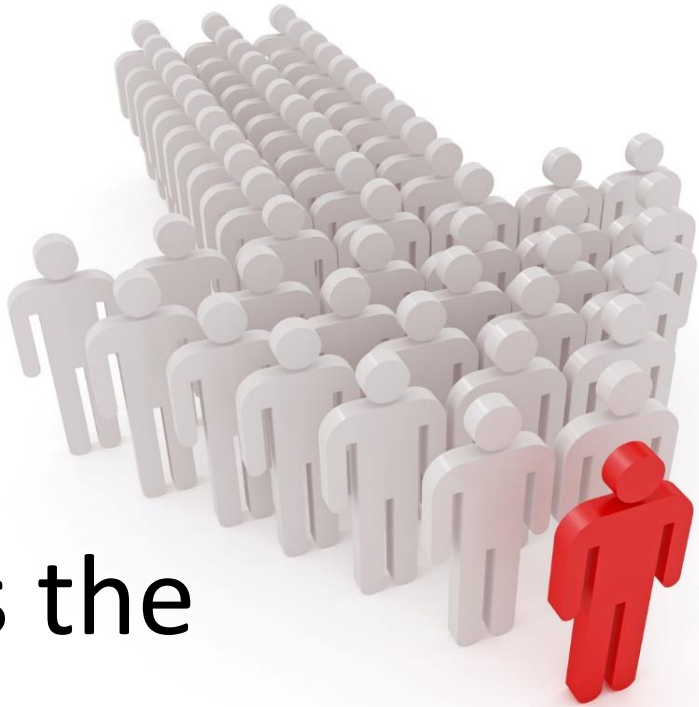
IT Steering Committee prioritizes IT actions

So, the project became as an opportunity for us to **share experiences** and to **exchange practices** among WGITA community

What is the GET.IT Project?

In 2013, WGITA meeting was held in the beautiful Vilnius, in Lithuania


INTOSAI
22nd Meeting of the INTOSAI Working Group on IT Audit
25-26 April 2013, Vilnius, Lithuania
I WAS THERE!



IT Governance was the #1 pick of the survey conducted with the WGITA community for the next work plan

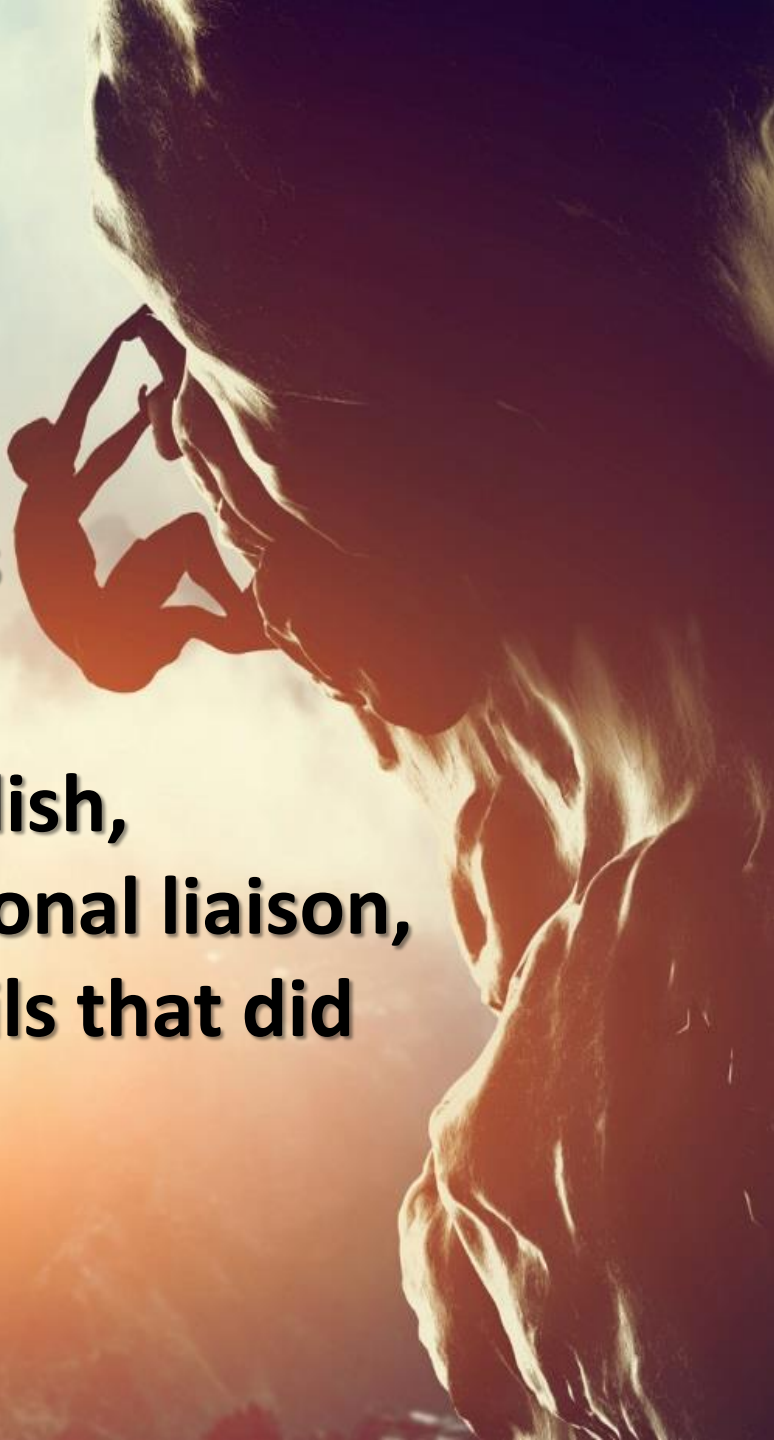
So, we decided to join efforts to produce a guide on IT Governance for our community

It was named

Participating SAIs

- Auditor-General of **South Africa**
- Federal Court of Accounts of **Brazil** (Project Leader)
- National Audit Office of **Lithuania**
- State Audit Bureau of **Kuwait**
- **US** Government Accountability Office (GAO)

Main challenges



- Combining different approaches and backgrounds
- Text harmonization
- Communication (written english, contacting the right international liaison, wrong e-mail adresses, e-mails that did not reach the right person)

The Project agenda needs to be balanced with internal work

RESULTS


GET.IT
Governance Evaluation
Techiniques for
Information Technology
A WGITA Guide
for Supreme audit
institutions
INTOSAI
Working Group on IT Audit
TCU FEDERAL COURT OF ACCOUNTS

SUMMARY

1.4 Principles of IT Governance (ISO/IEC 38500:2008 Standard)

The different definitions for IT governance, as mentioned on the previous sections, have originated several best practices and frameworks to guide the implementation of the related concepts in a given organization.

The ISO/IEC 38500:2008 standard provides guiding principles for directors of organizations (including owners, board members, directors, partners, senior executives and similar roles) on the effective, efficient and acceptable use of IT within their organizations.

It provides a framework of six IT governance principles that, if followed, aim to:

- provide stakeholders (including clients, shareholders, employees and the general public) with the necessary confidence to trust in the organization's governance of IT;
- inform and guide directors in the use of IT in their organizations;
- provide a basis for objective evaluation of the governance of IT within the organization.

Figure 1: IT governance principles (ISO/IEC 38500:2008)

These principles should then be translated into general guidelines concerning IT governance, as follows:

- Responsibility: establish clearly understood responsibilities for IT;
- Strategy: plan IT to best support the organization;
- Acquisition: acquire IT products and services validly;
- Performance: ensure IT performs well whenever required;
- Conformance: ensure IT complies with laws and rules;
- Human behavior: ensure IT respects human factors.

1.5 Key Elements of IT Governance

To accomplish the effective delivery of IT solutions, an organization needs to have some key IT governance elements in place. These elements are described next.

1.5.1 IT Strategy and Planning

IT Strategy represents the mutual alignment that is supposed to exist between business' and IT's strategic objectives. These last ones should consider the current and future needs of the business, the current IT capacity to deliver services and the requirement of resources (ISO/IEC 2008, p. 11) The strategy should integrate IT capabilities (infrastructure, delivery model, available resources, including staff etc.) into a common approach to support the business objectives.

Chapter 1. Concepts and definitions

GOVERNANCE EVALUATION TECHNIQUES FOR IT (GET.IT)

Chapter 02

Without a sound idea of how to effectively utilize IT resources, an organization risks wasting money and, more importantly, failing to meet its overall business objectives. Good IT governance implementation will increase the likelihood of success and will ensure that limited IT resources are well utilized.

Thus, auditors need to ensure that the audited entity has an effective IT governance framework in place. However, they need to keep in mind both the size of the organization and its mission. Large organizations should have most of the key elements in place. Audits in smaller organizations or audits of organizations whose mission is not as complex, in turn, may exclude from the evaluation some details of key elements.

Next sections describe four evaluation techniques that could be used by organizations in the public sector to assess properly IT governance, considering the targeted profile of the organization.

Chapter 2. Four evaluation techniques

2. NATIONAL AUDIT OFFICE OF LITHUANIA – THE STATE CONTROL

"STATE-LEVEL" AND "IT SELF-ASSESSMENT" METHODS

2.1 Summary

The National Audit Office of Lithuania (the NAO LT), accountable to the Seimas (the Parliament) has the mandate to audit each level of the government, starting from institutional level up to the state-level, when audit objective is extended to effectiveness and efficiency of implementation of IT policies, set by the Government. This allows the NAO LT to be active and competent adviser to the Government, suggesting the best IT governance practices, which are subsequently embedded to the national legislation.

The National Audit Office of Lithuania uses its own IT function to test and apply best practices, showing example to the public sector that audit recommendations may be practical, as cascade to develop reliable IT goals and performance criteria.

Having the wide audit scope, equipped with modern IT governance methods and practices which are tested and applied on the NAO LT before offered to the auditees, the competent IT audit staff is able to suggest the best possible options to improve IT governance at both institutional and the state levels. Acting this way, the NAO LT is active and competent adviser to the Government.

2.2 The SAI

The National Audit Office (the State Control) of Lithuania was established in 1919 and appoint-

Chapter 3. Four case studies

GET.IT

Governance Evaluation Techniques for Information Technology

The Document

A WGITA Guide for Supreme Audit Institutions

INTOSAI Working Group on IT Audit

TCU FEDERAL COURT OF ACCOUNTS

IT GOVERNANCE

Chapter 01

This chapter addresses some concepts regarding governance, as well as its relevance in the context of public organizations and their control, the role of information technology (IT) governance and its expected contributions to improving results in both the technology area and the core business of an organization.

The Evaluate-Direct-Monitor cycle describes the motor driving of value creation. Through these three activities, governance ensures that stakeholders' needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved, that direction is set through prioritization and decision-making and that performance and compliance are monitored against agreed-on direction and objectives (ISACA, 2012a, p. 31).

Risk analysis is an important piece of governance, including IT governance. Latter section in this chapter provides a set of common risks and an explanation of the possible consequences of failures in IT governance.

In the final section, a guide of the main enablers of good governance provided by COBIT 5 is described. Lack of enablers may affect the ability of the enterprise to create value.

Objective: Present concepts related to Governance so users can have the most relevant approaches in a single place

Figure 1: IT governance principles (ISO/IEC 38500:2008)

COBIT and ISO/IEC 38500 still are the main references to IT governance

Figure 2: The Evaluate-Direct-Monitor cycle and IT governance principles

4. ENABLERS OF IT GOVERNANCE

Enablers are factors that, individually or collectively, have the ability to influence the proper functioning of the organiza-

e the seven categories
n COBIT 5, as well as
blications address the

licies and

principles, policies and
eans by which gover-
on setting) are institu-
, they act as integrating
e decisions and man-
ion of decisions (ISACA,

erred behavior, set in
-making and, as such,
nust be demanded by
18, p. 6). Thus, all people

in the organization involved in the planning, management, operation or use of IT resources should make decisions and perform actions in observance of the established principles. The ISO/IEC 38500:2008 standard defines six principles for good corporate governance of IT: responsibility, strategy, acquisition, performance, conformance and human behavior.

Among others, examples of the principles of IT governance are the need for the organization's business strategy to take into account the current and future IT capabilities, the requirement that IT complies with applicable laws and regulations and the need for IT acquisitions to be made for valid reasons, balancing benefits, opportunities, costs and risks (ISO/IEC, 2008, p. 6).

In this context, in order that senior management may govern IT to meet institutional needs, it is necessary to establish a set of principles to guide the desired behavior in the management and use of institutional IT. It is noteworthy that, regarding public organizations, the principles for IT governance must be aligned with the general principles governing public administration

in an efficient manner. Nevertheless, while senior leadership is usually concerned with business strategy and strategic risks, few leaders have focused on IT issues, despite the fact that they involve large investments and huge risks. Why is that? Among the reasons: IT requires more technical insights than other disciplines in order to understand how it enables the enterprise and creates risks and opportunities; IT has traditionally been treated as an entity apart from the business; IT is complex, even more so in the context of an extended enterprise operating in a networked economy.

Thus, there is a need for mechanisms to ensure that IT be fully integrated into the business, **aligning** the direction of IT with the organization's objectives, **limiting risks** and ensuring that IT creates **business value**. Best governance practices provide guidance on such possible mechanisms, describing the role of top management in promoting and maintaining this alignment and helping them with tools **to evaluate, to direct and to monitor** the use of IT.

The implementation of IT governance principles is currently considered the preferred method to ensure effective, efficient, secure and acceptable use of IT within organizations.

1.1 Definitions of Governance

In essence, governance comprises the mechanisms of leadership, strategy and control put in place to evaluate, direct and monitor the performance of management towards the conclusion of stakeholders' goals and interests (TCU, 2014, p. 26).

Rachel M. Gisselquist, in a paper released in 2012, notes that "the term [governance] is widely used in relation to a variety of specific contexts and approaches: e.g., corporate governance, participatory governance, global governance, information technology governance, environmental governance, local governance, NGO governance, and sustainable governance" (Gisselquist, 2012, p. 5). Each type of governance follows specific sources of guidance, each with similar goals but, often, varying terms and techniques for their achievement.

Narrowing the perspective to the IT environment, according to Robert S. Roussey, "IT governance is the term used to describe how those persons entrusted with governance of an entity will consider IT in their supervision, monitoring, control and direction of the entity. How IT is applied within the entity will have

And other quotes come in the same way

1.2 IT Governance as Part of Corporate Governance

IT governance is a key component of the overall corporate governance of the organization. It should be regarded as how IT creates value that fits into the corporate strategy, and never

1.3 Importance of IT Governance

Understanding the reasons that call for IT governance in an organization gives more clarity to its importance. Generally, there will be

GOVERNANCE EVALUATION TECHNIQUES FOR IT (GET.IT)

Chapter 02

Without a sound idea of how to effectively utilize IT resources, an organization risks wasting money and, more importantly, failing to meet its overall business objectives. Good IT governance implementation will increase the likelihood of success and will ensure that limited IT resources are well utilized.

Thus, auditors need to ensure that the audited entity has an effective IT governance framework in place. However, they need to keep in mind both the size of the organization and its mission. Large organizations should have most of the key elements in place. Audits in smaller organizations or audits of organizations whose mission is not as complex, in turn, may exclude from the evaluation some details of key elements.

Next sections describe four evaluation techniques that could be used by organizations in the public sector to assess properly IT governance, considering the targeted profile of the organization.

Objective: present evaluation techniques useful to different types of SAIs objectives

1. AUDITING INDIVIDUAL ORGANIZATIONS

Audit Objectives

Audit Objective (1) Business Needs Identification, Direction and Monitoring

Audit Objective (2) IT Strategy

Audit Objective (3) Organizational Structures, Policy and Procedures

Audit Objective (4) People and Resources

Audit Objective (5) Risk Assessment and Compliance Mechanisms

1.8 Auditing a Large Entity

The WGITA Handbook on IT Audit described some of the risks and organization faces if they do not have a well-defined IT governance implementation. As an IT Auditor, we need to look at whether they have addressed those

1.9 Auditing a Smaller Entity

Smaller entities may not have all of the resources to implement all aspects of IT Governance as a larger organization. Nevertheless, they do have resources constraints and must strive to ensure that IT resources are effectively

Related Audit Issues:

- **Defining IT requirements:** How does the organization identify and approve business and IT requirements?
- **Leadership** rect and mo ness and IT
- **IT Investm** tion manag

Related Audit Issues:

- **Quality of IT strategy:** Does the organization have an IT Strategy that serves to guide its IT functions?
- **Risk managemen** zation manage the

Related Audit Issues:

- **HR and logistics:** How does the organization deal with meeting current and future people and resource requirements?

2. STATE-LEVEL / PERFORMANCE AUDITING

2.2 State-level IT Assurance Framework

Within the context of the public sector, the roles of the three-party components can be mapped as follows:

- **An accountable party:** in the most of the countries should be the Government;
- **The user:** should be the legislative body (Parliament), citizens and other stakeholders;
- **The assurance professional (auditor):** is the SAI or the Auditor General.

2.3 Public Sector's Perspective of IT Governance

- Board of Directors / Executive Authority
- Senior / Executive Management
- Audit Function

2.4.1 Evaluation of Public Entities Internal Control

2.4.2 Evaluation in Terms of Economy, Efficiency, Effectiveness (3E) / IT 3E Audits

2.5 State-level / Performance Audit Considerations

In order to develop a government-wide performance audit plan on IT governance, the information obtained should then be analyzed in terms of the following:

- Macro environment;
- Government objectives;
- Audit outcomes;
- Requests for audits from oversight bodies.

3. SURVEY-BASED AUDIT

3.1.1 What is the Method?

The method consists of appraising the general situation of a large group of organizations that are subject to audits from the surveyor entity by gathering unavailable information from each in a standardized, easily comparable way.

Pros: scalability to hundreds of organizations, simultaneously; efficiency in employed resources;

can pro

tion; ea

Limitations: reliability of collected responses (ambiguity in the interpretation of the questions; noisy data from miscommunication-

need t

to veri

Difficulties: effective communication through a questionnaire (write clear unambiguous questions that can be universally understood in a similar way despite considerable organizational variance in governance maturity and

Figure 4: IT governance profile survey

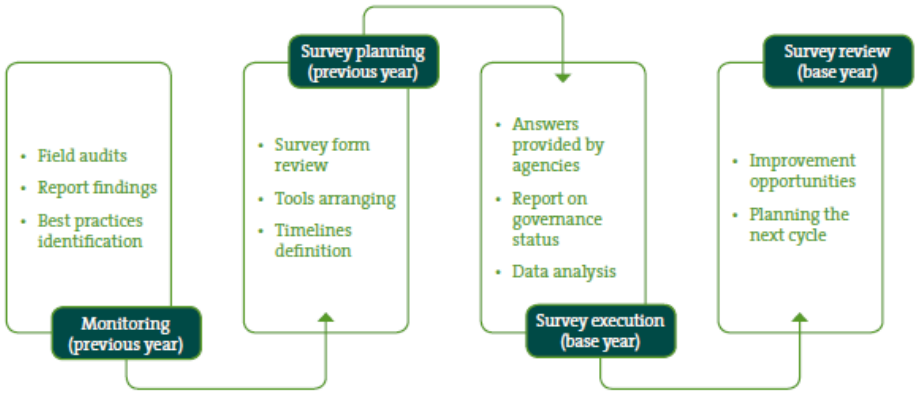


Table 1: IT Governance Survey

Concerning the IT governance system:	Adoption level of the practice				
	Doesn't apply	Not adopted	Initiated a plan to adopt	Partially adopted	Entirely adopted
The organization defines and communicates formally roles and relevant responsibilities to governance and IT management.					
The organization have an IT committee formally established, composed by agents of its relevant areas.					
The committee performs the expected activities on its constitutive act.					
The organization prioritizes the IT actions with the support of the IT committee (or equivalent collegiate), which acts as advisory instance for the high administration.					

4. IT SELF-ASSESSMENT

Developed by EUROSAI ITWG, **Methodology for IT self-assessment for SAIs** (EUROSAI IT Working Group, 2007):

- uses CMM-based COBIT process assessment model;
- suggests how organization-specific Goals cascade has to be built, exploring business goals, prioritizing them, then linking appropriate COBIT processes – those having major impact on achievement of business goals – and analyzing process maturity issues.

The method consists of two parts:

- the **Methodology for IT self-assessment for SAIs**, describing how to organize self-assessment workshops, how to related business and COBIT processes, how to measure current and to set future maturity levels and how to transform maturity gaps into measurable IT projects intended to cover those maturity gaps) and uses CMM-based COBIT maturity model;
- Practical self-assessment workshops, moderated by external experts where representatives of business and IT functions of

Stage 1: Organization of the IT Self-assessment

Stage 2: Preparation for the Pre-workshop Meeting

Stage 3: Pre-workshop Meeting (4h)

Stage 4: Preparation for the Workshop

Stage 5: Workshop [7h30min; shall be split in two days: (a)-(d) + (e)-(g)]

4.1.4.1 Pros

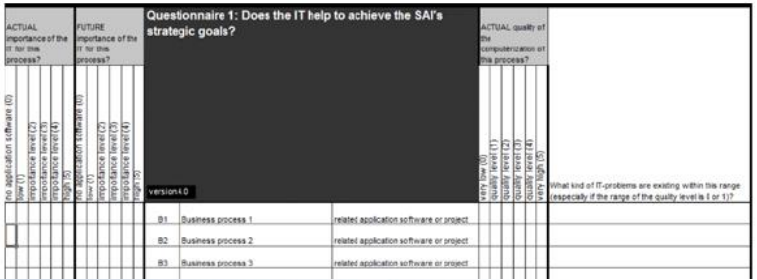
4.1.4.2 Limitations

- The method has no major limitations – the ma… ne… ces… ces…

4.1.4.3 Difficulties

- Requires knowledge of COBIT processes and control objectives, sometimes it is a problem for key business people;

Figure 5: BVC form



Chapter 03

CASE STUDIES

The purpose of this chapter is to present some case studies of actual audits performed by the participating SAIs. These case studies were selected to demonstrate the utilization of the four audit methods discussed in the previous chapter.

The corresponding audits were performed by four SAIs, as follows:

I. An audit of a healthcare information system (HIS) performed by the State Audit Bureau of Kuwait using the "Individual Organization" method;

II. A state-level IT governance audit performed by the National Audit Office of Lithuania using the "State-level" and "IT Self-assessment" methods;

III. A means of promoting IT governance performed by the Federal Court of Accounts of Brazil using the "Survey-based" method;

IV. Implementation of a corporate governance of information and communication technology policy framework performed by the Auditor-General of South Africa using the "Individual Organization" method.

Each case study starts with a summary and, after a brief introduction describing the author SAI, is presented in four sections:

- The Challenge: describes the problem related to IT governance;
- What Was Done: depicts the SAI's approach on IT governance evaluation and audit;
- Evolution: how the situation evolved after the SAI's actions and what were the main contributions resulting from the adopted approach;
- Key Messages: brings the main aspects that could be generalized to help other SAIs.

Objective: Demonstrate the utilization of the four evaluation techniques by participating SAIs

NATIONAL AUDIT OFFICE OF LITHUANIA – THE STATE CONTROL

"STATE-LEVEL" AND "IT SELF-ASSESSMENT" METHODS

> "Having the wide audit scope, equipped with modern IT governance methods and practices which are tested and applied on the NAO LT before offered to the auditees, the competent IT audit staff is able to suggest the best possible options to improve IT governance at both institutional and the state levels. Acting this way, the NAO LT becomes a competent adviser to the Government."

STATE AUDIT BUREAU OF KUWAIT

"INDIVIDUAL ORGANIZATION" METHOD

> "The State audit Bureau of Kuwait has initiated an IT Governance audit on a healthcare information system (HIS) that is to be replaced. The (HIS) belongs to a hospital that serves the employees and their families of the country's national oil company and its 11 subsidiaries."

AUDITOR-GENERAL OF SOUTH AFRICA

"INDIVIDUAL ORGANIZATION" METHOD

> "A directive was also issued to all departments and organs of state to implement the CGICTPF in three structured phases over three years and the final date for full implementation is March 2016 (DPSA, 2013b). The CGICTPF implementation guidelines, together with the conformance and performance assessment standards, were developed by the DPSA, in collaboration with the Department of Performance Monitoring and Evaluation (DPME). The deliverables of phase 1 were due in March 2014."

FEDERAL COURT OF ACCOUNTS OF BRAZIL

"SURVEY-BASED" METHOD

> "The Federal Court of Accounts of Brazil (Tribunal de Contas da União – TCU) has been playing an active role on the promotion of IT governance within Brazilian public institutions and agencies. Through an iterative process combining surveys, audits and pedagogical actions, there is a growing perception by the management space regarding the need for stronger processes under the IT environment."

Before finishing... Special thanks to...

- Mr. Phere Motau – SAI South Africa
- Mr. Erick Muzart, Regis Machado, Marcio Braz and Diego Hulse – SAI Brazil
- Mr. Dainius Jakimavicius – SAI Lithuania
- Mr. Osama Alfaris and Mr. Saad Alkafan – SAI Kuwait
- Mr. Madhav Panwar – SAI USA

TRIBUNAL DE CONTAS DA UNIÃO

Thank you!

sefti@tcu.gov.br