

GET.IT

Governance Evaluation
Techniques for
Information Technology

*A WGITA Guide
for Supreme Audit
Institutions*



INTOSAI
Working Group on IT Audit



FEDERAL COURT OF ACCOUNTS



Federative Republic of Brazil

Federal Court of Accounts

MINISTERS

Aroldo Cedraz de Oliveira, President

Raimundo Carreiro, Vice-President

Walton Alencar Rodrigues

Benjamin Zymler

Augusto Nardes

José Múcio Monteiro

Ana Arraes

Bruno Dantas

Vital do Rêgo

SUBSTITUTE MINISTERS

Augusto Sherman Cavalcanti

Marcos Bemquerer Costa

André Luís de Carvalho

Weder de Oliveira

PUBLIC PROSECUTION OFFICE OF TCU

Paulo Soares Bugarin, Prosecutor General

Lucas Rocha Furtado, Assistant Prosecutor

Cristina Machado da Costa e Silva, Assistant Prosecutor

Marinus Eduardo de Vries Marsico, Prosecutor

Júlio Marcelo de Oliveira, Prosecutor

Sérgio Ricardo Costa Caribé, Prosecutor

Governance Evaluation Techniques for Information Technology

GET.IT

© Copyright 2016, Tribunal de Contas da União
<http://www.tcu.gov.br>
SAFS, Quadra 4, Lote 1
CEP: 70042-900 | Brasília/DF

The complete or partial reproduction
of this publication is permitted, without
altering its content, as long as the source is
cited and it is not for commercial purposes

Internacional Organization of Supreme Audit Institutions
(Intosai). Working Group of Information Technology (WGITA).

Get.it : governance evaluation techniques for information
technology : a WGITA guide for supreme audit institutions. – Brasília
: Federal Court of Accounts of Brazil, 2016.

130 p.

1. Information technology. 2. Governance. 3. Information
technology audit. I. Title.

Catalogued by Biblioteca Ruben Rosa

GET.IT

Governance Evaluation
Techniques for
Information Technology

*A WGITA Guide
for Supreme Audit
Institutions*

Brasília, 2016



PREFACE



The background image is a composite of a city skyline and a bar chart. The bar chart has a y-axis with values 0.00, 2.50, 5.00, and 7.50. The x-axis has labels for the years 2014, 2015, and 2016. The bars show a general upward trend. A large, semi-transparent green arrow points from the bottom left towards the top right, passing over the bar chart. A diagonal line runs from the top left corner to the bottom right corner, separating the dark blue background from a solid green area on the right. The word 'PREFACE' is written in white, sans-serif capital letters in the upper left quadrant.

The Federal Court of Accounts of Brazil (TCU) joined the INTOSAI Working Group of Information Technology (WGITA) in 1996, ten years before the creation of the Department of External Control – Information Technology (Sefti), a technical unit specialized in the topic.

Our involvement in the debates and the knowledge developed in the works carried out by the group has enabled our team of auditors to quickly build their capacity and was essential for TCU's advancement of information technology (IT) auditing in the Public Administration.

In this regard, this guide, coordinated by TCU, is one more step in our commitment with INTO-SAI partners, reaffirming section 17 of the Lima Declaration, which was a result of the process initiated in 2007 with the purpose of inducing adoption of IT best practices by the Public Administration. This was done through specific surveys aimed at evaluating the context of leadership, strategy, risk management and ac-

countability in organizations and in public policies in the area of Information Technology.

I would like to highlight what we learned because of the Coordinated Audit in IT Governance, led by TCU between 2014 and 2015, within the scope of the Organization of Latin American and Caribbean Supreme Audit Institutions (OLACEFS). In that occasion, we observed the enthusiasm of the participants with the knowledge shared and, later, with the first results observed. Thus, I have no doubt in recommending capacity building in the proposed topic and the application of the techniques listed in their respective control actions.

Finally, I must state that the described concepts and methods are not an end in themselves. They seek to improve Public Administration, to attain more rationality in processes, to promote a culture of planning and monitoring of governmental actions in order to make application of public resources compatible with the urges of the citizens, which is something that all Supreme Audit Institutions pursue.

Brasília, March 10, 2016

AROLDO CEDRAZ DE OLIVEIRA

President of TCU

```
webSecurity.TrackLocation();
```


TEAM MEMBERS OF WGITA GET.IT GUIDE PROJECT

Auditor General of South Africa

- Mr. Phere Motau, Technical Manager – Audit Research and Development

Federal Court of Accounts of Brazil

- Mr. Diego Hülse, Auditor
- Mr. Erik Muzart Fonseca dos Santos, Auditor
- Mr. Marcio Rodrigo Braz, Chief of Department of External Control - IT
- Mr. Regis Soares Machado, Auditor

National Audit Office of Lithuania

- Mr. Dainius Jakimavičius, Advisor to the Auditor General

State Audit Bureau of Kuwait

- Mr. Osama AlFaris, Information Technology Audit Controller
- Mr. Saad AlKalfan, Senior Information Technology Auditor

US Government Accountability Office

- Mr. Madhav Panwar, Senior Level Technologist – Director

GLOSSARY OF ACRONYMS AND ABBREVIATIONS

- **AGSA** Auditor-General of South Africa
- **APP** Annual Performance Plan
- **BVC** Business Value Chain
- **CGICTPF** Corporate Governance of Information and Communication Technology Policy Framework
- **CIO** Chief Information Officer
- **CIPFA** Chartered Institute of Public Finance and Accountancy
- **CMM** Capability Maturity Model
- **COBIT** Control Objectives for Information and Related Technology
- **COSO** Committee of Sponsoring Organizations of the Treadway Commission
- **DPME** Department of Performance Monitoring and Evaluation
- **DPSA** Department of Public Service and Administration
- **EDM** Evaluate, Direct and Monitor
- **FAQ** Frequently Asked Questions
- **FOSAD** Forum of South African Director Generals
- **GAO** United States Government Accountability Office
- **GET.IT** Governance Evaluation Techniques for IT
- **GITOC** Government Information Technology Officer's Council
- **HIPAA** Health Insurance Portability and Accountability Act
- **HIS** Healthcare Information System
- **HR** Human Resource
- **ICGGPS** Independent Commission for Good Governance in Public Services
- **ICT** Information and Communication Technologies
- **IFAC** International Federation of Accountants
- **iGovTI** IT Governance Scoring
- **IIA** Institute of Internal Auditors

- **INTOSAI** International Organization of Supreme Audit Institutions
- **ISA** Information Systems Auditing
- **ISACA** Information Systems Audit and Control Association
- **ISACF** Information Systems Audit and Control Foundation
- **ISO/IEC** International Organization for Standardization / International Electrotechnical Commission
- **IT** Information Technology
- **ITGI** IT Governance Institute
- **ITGP** IT Governance Policy
- **ITIL** Information Technology Infrastructure Library
- **ITSA** IT self-assessment
- **MEA** Monitor, Evaluate and Assess
- **MFMA** Municipal Finance Management Act
- **Minport** Ministerial portfolio
- **MPAT** Management Performance Assessment Tool
- **MPSA** Minister of Public Service Administration
- **NAO** National Audit Office of Lithuania
- **OPM** Office for Public Management Ltd
- **PAA** Public Audit Act
- **PFMA** Public Finance Management Act
- **PSICTM** Public Service ICT Management
- **ROI** Return On Investment
- **SAI** Supreme Audit Institution
- **SAB** State Audit Bureau of Kuwait
- **SCoAG** Standing Committee on the Auditor-General
- **Sefti** TCU's Department of External Control - IT (in portuguese: *Secretaria de Fiscalização de TI*)
- **TCU** Federal Court of Accounts of Brazil
- **WGITA** Working Group on IT Audit
- **3E** Economy, Efficiency, Effectiveness

SUMMARY

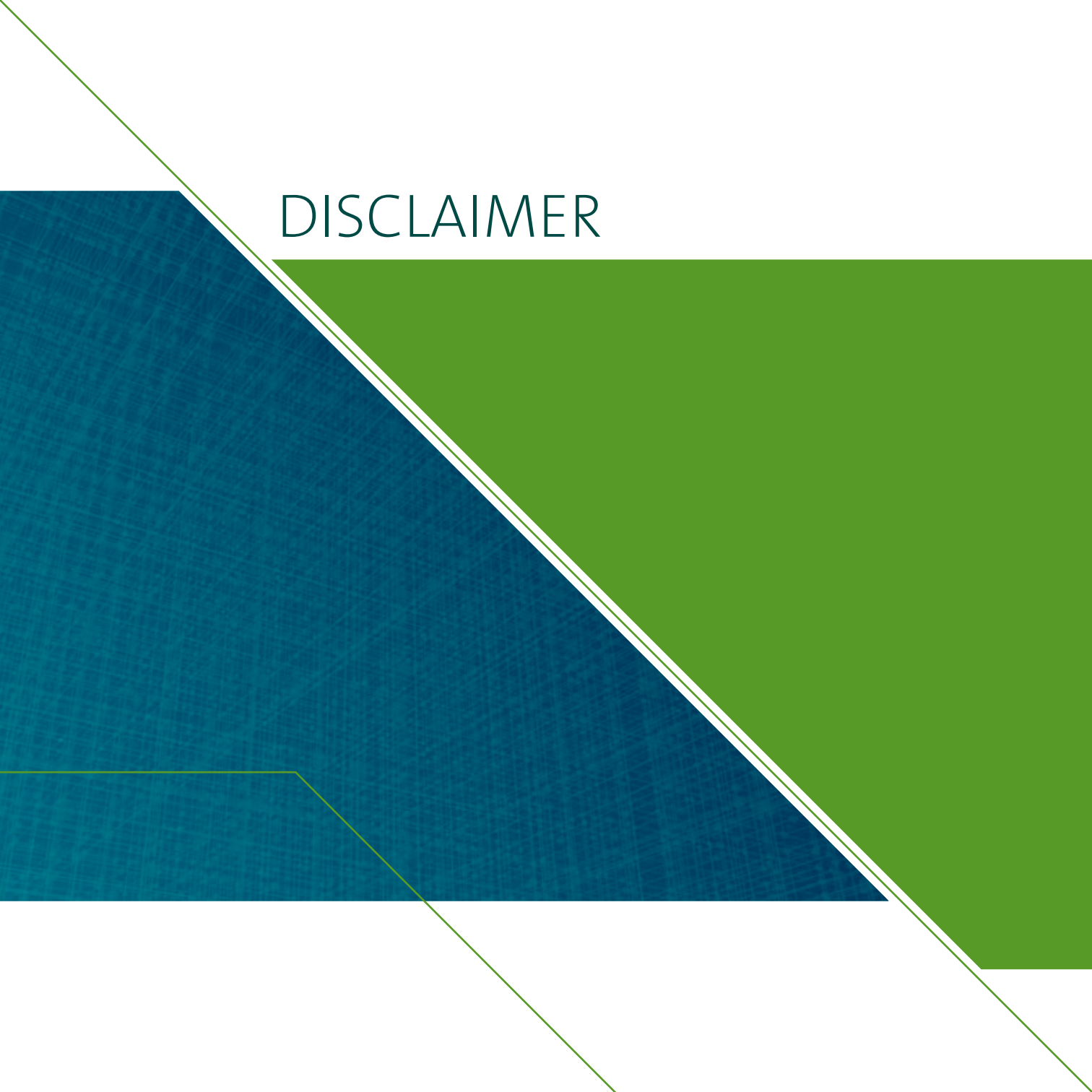
DISCLAIMER	12		
INTRODUCTION	14		
CHAPTER I		CHAPTER III	
IT GOVERNANCE	16	CASE STUDIES	98
1. Introduction to Governance	18	1. State Audit Bureau of Kuwait: <i>"Individual Organization" method</i>	100
2. The Evaluate-Direct-Monitor Cycle	27	2. National Audit Office of Lithuania – The State Control: <i>"State-level"</i> and <i>"IT Self-assessment" methods</i>	107
3. Risks and Consequences	31	3. Federal Court of Accounts of Brazil: <i>"Survey-based" method</i>	114
4. Enablers of IT Governance	33	4. Auditor General of South Africa: <i>"Individual Organization" method</i>	119
CHAPTER II		REFERENCES	127
GOVERNANCE EVALUATION TECHNIQUES FOR IT (GET.IT)	42		
1. Auditing Individual Organizations	44		
2. State-level / Performance Auditing	56		
3. Survey-based Audit	67		
4. IT Self-assessment	77		

LIST OF FIGURES

• Figure 1: IT governance principles (ISO/IEC 38500:2008)	23
• Figure 2: The Evaluate-Direct-Monitor cycle and IT governance principles	27
• Figure 3: Performance audit process	64
• Figure 4: IT governance profile survey	70
• Figure 5: BVC form	93
• Figure 6: COBIT form	94
• Figure 7: Findings and actions form	95
• Figure 8: Sample BVC consolidation form	95
• Figure 9: Sample COBIT consolidation form	96
• Figure 10: ICT house of value	119
• Figure 11: Oversight structure for corporate governance of ICT in public service	120

LIST OF TABLES

• Table 1: IT Governance Survey	74
• Table 2: IT Risks Survey	74
• Table 3: Information Security Survey	75
• Table 4: Assessment Levels	125



DISCLAIMER



The objective of the Governance Evaluation Techniques for IT (GET.IT) guide is to share with the wider INTOSAI community good IT audit practices, methods and tools regarding IT Governance which were successfully applied by the Supreme Audit Institutions (SAIs) that participated on this project. The purpose is to encourage other SAI members to take advantage of them and freely select, apply, adjust to their national contexts and, finally, institutionalize the practices.

The GET.IT guide is not meant to revise or replace the INTOSAI Handbook on IT Audit for Supreme Audit Institutions on the topic, but, instead, to complement and support it, highlighting its vitality and practical applicability to local contexts.

The GET.IT guide should not be taken as the universal truth, but as an additional instrument that contributes to widen the discussion on the theme. In this sense, agreeing, disagreeing and finding alternative and proper ways regarding the application of emerging good practices to country-specific realities are highly encouraged, as well as the subsequent sharing of these experiences with others.



INTRODUCTION

The background of the slide is split diagonally from the top-left to the bottom-right. The upper-left portion is dark blue and contains a faint, semi-transparent financial chart. This chart includes a candlestick pattern, a triangular volume indicator, and a line graph. Faint numerical values like '2009', '2010', '25', '50', and '75' are visible on the chart. The lower-right portion is a solid, vibrant green. A thin white double-line border separates the two colored regions. A thin green line runs diagonally across the entire slide, parallel to the main split.

Fast information society development, supported by the rise of the Internet, E-Government and E-Commerce, emitted numerous good practices. These practices have been generalized and consolidated by existing and emerging

IT governance models and standards, as a counterweight for corporate setbacks and failures and stakeholders' concern about proper and professional management of their interests. The models and standards are being both interdependent and diverse to provide clear guidance for regulatory frameworks for information technology to unfold its full potential.

Traditionally, IT audit function only aimed to assure compliance with legal acts. At present, it is used to provide independent and professional advice on IT governance issues.

Good practices, selected and applied wisely for IT governance at institutional and state levels, influenced significantly on the growth of IT audit, which has already outgrown its original mission of performing attestation services for accounting systems and became a powerful instrument for value-for-money audits.

With diversity of national IT governance objectives and regulatory frameworks, good practices for IT governance remain being stable audit criteria, against which initiatives of the Government are assessed in terms of economy, effectiveness and efficiency.

Being in a good position to monitor the public sector development and having the power to issue recommendations to advice the Government to implement new forms of better governance, the Supreme Audit Institution has to pay primary attention to the development of the IT audit function, taking into consideration its mandate and the importance of IT in the public sector.

Applying the same auditing standards, having the same client – the government sector – and having the same objective – to suggest improvements to its performance – Supreme Audit Institutions have a lot of similarities, while the difference in methods and tools should encourage them to share ideas and knowledge in order to find the best solutions.

Knowledge Sharing: this is probably the fundamental potential of cooperation. When best practices are collected, refined and employed, it enables the use of all the aggregated knowledge and experience to find the most suitable solutions.

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.

1. INTRODUCTION TO GOVERNANCE

Most organizations use information technology (IT) as an essential business tool and few can function without it. IT is fundamental for managing organization resources, dealing with suppliers and customers, and enabling increasingly global and dematerialized transactions. IT is key for recording and disseminating business knowledge. In addition, IT also plays a significant role in the future business plans of many organizations.

An ever-larger percentage of the organization value has transitioned from tangible (inventory, facilities etc.) to intangible (information, knowledge, expertise, reputation, trust, patents etc.) assets, many of which revolve around the use of IT. Therefore, reliable and consistent IT results are critical in supporting and enabling organizational goals (ITGI, 2003, p. 13).

Despite significant financial and organizational investments, many IT projects and IT supported business projects end up failing or returning less than expected to the organization. IT related acquisitions are fraught with problems. Inadequate IT systems can hinder the performance and

competitiveness of organizations and expose them to the risk of not complying with legislation or other contractual obligations.

It is clear that, in these days of doing business on a global scale around the clock, system and network downtimes have become far too costly for any organization to afford. In some industries, IT is a mandatory resource to differentiate the organization from its competitors and provide it with a competitive advantage. In many others, more than just prosperity, it determines the organization's survival itself.

The networked economy has increased the efficiency of the markets, enabled streamlining of processes and optimized supply chains. It has also created new technology and business risks and new information and resilience requirements. These new risks and requirements demand a more effective and transparent management of IT.

For an organization with limited resources to expend on IT, it is critical that projects be defined, selected, built (or bought) and operated

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

an immense impact on whether the entity will attain its vision, mission or strategic goals” (ITGI, 2003, p. 1). In other words, IT governance, which is the responsibility of the board of directors and executive management, comprehends the necessary mechanisms, such as leadership, organizational structures and processes, which combined should “ensure that the organization’s IT sustains and extends the organization’s strategies and objectives” (ITGI, 2003, p. 10), helping it meet its goals today and incorporate plans for future needs and growth.

In an audit and control related perspective, governance mechanisms can be applied to ensure that IT service providers are sufficiently transparent, have adequate controls, and provide the information necessary for the organization to properly and independently assess and monitor the efficacy of those controls. IT governance plays a key role in establishing a sound control and reporting environment for management oversight and review (INTOSAI, 2014, p. 18).

This concern over governance is particularly pronounced in the case of public organizations. Having several institutions addressing the theme, assessing the conditions necessary

for improving governance in their own contexts, they agreed that, in order to best serve the interests of society, it is important to ensure several controls: ethical, responsible, committed and transparent leadership behavior; corruption controls; effective implementation of a code of conduct and ethical values; compliance to regulations, codes and standards; transparent and effective communications; effectively engaged stakeholders (citizens, service users, shareholders, private enterprises), with balanced interests. Examples of such institutions include the International Federation of Accountants (IFAC), the Chartered Institute of Public Finance and Accountancy (CIPFA), the Office for Public Management Ltd (OPM), the Independent Commission for Good Governance in Public Services (ICGGPS), the World Bank and the Institute of Internal Auditors (IIA).

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

be seen as a discipline on its own. In taking this approach, all stakeholders would be required to participate in the decision-making process. This creates a shared acceptance of responsibility for critical systems and ensures that IT-related decisions are made and driven by the business and not the opposite (INTOSAI, 2014, p. 19).

For IT governance to ensure both that investments in IT generate business value and IT risks are properly mitigated, it is essential to put in place an organizational structure with well-defined roles for the responsibilities regarding information, business processes, applications and infrastructure.

It is also essential that IT governance ensure that stakeholders, business owners and other users, maintainers, operators etc. are involved with identifying new or updated business needs and then providing the organization with the appropriate IT (and non-IT) solutions in order to cope with those needs. During the development or acquisition of solutions to a particular business need, IT governance should ensure that the selected solutions are responsive to the business and that necessary training and resources (hardware, tools,

network capacity etc.) are available to implement them. Monitoring activities may be carried out by internal audit or quality assurance departments, which would periodically report to management.

The IT governance structure must be defined in order to assure that the IT decisions, directions, resources, management and monitoring support the organization's strategies and objectives.

In summary, IT governance stems from corporate governance but with its own specialization. It provides transparency and oversight of IT by means of the culture it promotes and its inherent organization, policies and practices. Proper IT risk management, direction and straightforward communications reduce cost and mitigate damages caused by IT pitfalls. It also promotes trust, teamwork and positivity in the use of IT and the people working on it.

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

an understatement of the IT potential by the business along with a misunderstanding of what the business requires from the IT side. Thus, it is a good practice that business establishes the knowledge of the IT potential and its benefits to the business.

Commonly, there would be a lack of joint accountability ownership between the IT users and the provider, which does not promote the success of IT services and projects.

The practice of benchmarking with standards and other organizations is an important issue for management. Additionally, management would also want to know how competent its current IT infrastructure is in supporting the business goals.

IT risk management is a subject that needs to be well communicated and understood by management. Since the adaptation of IT into the business is continually growing, all the inherent risks of using IT must be very well managed in order to support the decision-making process. It is a fact that IT is very unique in its nature of development and complexity. Thus, a strong foundation of management skills is needed.

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 governing the use of IT in their organization; and
- 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 conforms with formal 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 a series of factors (existing IT infrastructure and architecture, investments, delivery model, available resources, including staff etc.) into a common approach to support the business objectives.

It is important for the IT auditor to review the entity's IT strategic plans in order to assess the extent to which IT governance mechanisms have been embedded on the corporate decision-making process in regard to making IT-related decisions and defining the IT strategy itself.

1.5.2 Organizational Structures, Standards, Policies and Processes

Organizational structures are a key element of IT governance in articulating the roles of the various management and governance bodies across the business and decision-making process. They should assign clearly defined delegation of duties regarding decision-making and performance evaluation and monitoring. Organizational structures must also be supported by appropriate standards, policies and procedures, which should enhance the organization's decision-making capacity.

Organizational structures are influenced by the stakeholders, i.e. all groups, organizations, members or systems who affect or can be affected by an organization's actions. Examples of important external stakeholders for public organizations include the Parliament, the Congress, other Government entities and the citizens.

Organizational structures are also influenced by the users, both internal and external.

Internal users are the business executives, functional departments who own business processes and individuals within the organization who interact with business processes. External users are the agencies, individuals and others who use products or services provided by the organization (for example, other departments, citizens etc.). Another influence on organizational structures are the providers, i.e. companies, units or persons, both internal and external, who provide services to the organization.

1.5.2.1 IT Organizational Structure's Common Functions

1.5.2.1.1 IT Steering Committee

This is the central piece of the organizational structure. It comprises members of top and senior management and has the responsibility for reviewing, endorsing and committing funds for IT investments. The Steering Committee should be instrumental in devising business decisions for which technology should be provided to support business investments as well as approving how to acquire this technology. Investment

decisions involving “build vs. buy” solutions are the responsibility of the IT Steering Committee generally after suitable recommendations from designated groups or committees.

A Steering Committee may take on several forms and responsibilities within the organizations. It may be a group of senior executives appointed by the board to ensure that the board is involved in, and kept informed of, major IT-related matters and decisions (called Strategy Committee) or a group of stakeholders and experts who are accountable for guidance of programs and projects (ISACA, 2012a, p. 76).

Finally, the Steering Committee plays a critical role in promoting the necessary buy-in and providing management support for programs that entail changes to the organization.

In many public sector organizations, IT Steering Committee functions are part of the management function.

1.5.2.1.2 Chief Information Officer (CIO)

A senior person who is responsible for the management and operation of the organization's IT capabilities. In many public sector

organizations, the functions carried out by the CIO may be conducted by a group or department that has the necessary responsibilities, authority and resources.

1.5.2.2 Standards, Policies and Processes

Standards and policies are adopted by the organization and approved by senior management. Policies lay the framework for daily operations in order to meet the goals set by the governing body. Policies are supported by procedures and/or processes that define how the work is to be accomplished and controlled. These goals are set by senior management in order to accomplish the organization's mission and at the same time to comply with regulatory and legal requirements. Policies and corresponding procedures need to be communicated to all relevant users in the organization on a periodic basis. Standards and policies guide the day-to-day work of the organization. Standards document a unified way of, for example, coding software; policies assist in ensuring that the organization's personnel follow a consistent approach regarding doing their work. For example, a security policy might require periodic password change, a human resource (HR) policy might require minimum training hours per year etc.

Some of the key policies that guide the IT governance include:

1.5.2.2.1 Human Resource Policy

The HR policy deals with the hiring, training, job termination and other organization's HR functions. It deals with the roles and responsibilities of the various personnel within the organization as well as with the definition of the set of skills and/or training they are required to possess to carry out their duties. The HR policy is also concerned with the segregation of duties between the roles and responsibilities it assigns.

1.5.2.2.2 Documentation and Document Retention Policies

Documentation of information systems, applications, job roles and reporting systems, especially when periodically updated, is an important reference point to align IT operations with business objectives. Appropriate documentation retention policies enable tracking and managing iterative changes to the organization's information architecture.

1.5.2.2.3 Outsourcing Policy

IT outsourcing is most often aimed at allowing the entity's management to concentrate their efforts on core business activities. The need for outsourcing may also be driven by the need to reduce running costs. An outsourcing policy ensures that proposals for outsourcing operations, functions, databases and so on are developed and implemented in a manner that is beneficial to the organization. The outsourcing policy may at times be merged with the overall acquisition policy.

1.5.2.2.4 IT Security Policy

This policy establishes the requirements for protection of information assets, and may refer to other procedures or tools on how these will be protected. The policy should be available to all employees responsible for information security, including users of business systems who have a role in safeguarding information (personnel records, financial data etc.).

2. THE EVALUATE-DIRECT-MONITOR CYCLE

According to the ISO/IEC 38500:2008 standard, the establishment of IT governance on an organization is structured on a cycle consisting of three core activities aimed at driving the information technology towards the fulfilment of the stakeholders' needs.

These three activities encompass assessing the current and future use of IT, direct the implementation of plans and policies to ensure IT meets organizational goals and monitor performance against plans.

Therefore, the implementation of good IT governance involves performing these three tasks under the scope of the different IT governance principles.

Leaders must continually assess the current and future use of IT considering the adopted strategies, stakeholders' needs, technological changes, pressures, social and economic trends. From the **evaluation** of the current situation, changing trends and future business needs, it is possible to better define the direction to be taken (ISO/IEC, 2008, p. 7).

After the assessment, the leadership must define responsibilities and require the implementation of plans and policies in accordance with the established **direction**. These plans will then determine the flow of investments to projects and IT operations. This also includes taking the necessary steps to ensure that changes are properly planned and managed in order to

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



maximize outcomes and minimize interruptions to the business (ISO/IEC, 2008, pp. 7-8).

Leaders must also adequately **monitor** strategies, plans and projects to ensure that performance is in line with business objectives and expectations. Furthermore, it is also necessary to monitor compliance with external and regulatory obligations (ISO/IEC, 2008, p. 8).

Therefore, the continuous unfolding of this cycle, based on evaluate, direct and monitor activities, allows the proper management of resources in order to support the business' objectives and the stakeholders' needs.

The COBIT 5 framework, which consists of a set of international best practices in IT governance and management, also uses a similar approach. It has a specific domain of IT governance processes, called EDM (Evaluate, Direct and Monitor), which includes practices and activities directed to the evaluation of strategic options in establishing the IT direction and monitoring the results achieved.

The primary purpose of governance according to COBIT 5 is to **create value** for the stakeholders. Thus, the framework establishes governance

processes around three axes, interlinked to ensure **benefits delivery** by optimizing the use of available **resources** while sustaining acceptable levels of **risk**.

To ensure the **delivery of benefits** it is necessary to "optimise the value contribution to the business from the business processes, IT services and IT assets resulting from investments made by IT at acceptable costs" (ISACA, 2012b, p. 35). In summary, it is expected that the return arising from investments made in IT be maximized. In addition, to do so, it is necessary to establish activities aiming at assessing IT investments in order to ensure the prioritization of those that present the best relationships between their cost and the benefits they deliver. Still, regardless of prioritization, it is necessary to ensure that the organization does not carry out investments in projects or solutions whose returns do not meet minimum acceptable levels.

On the other hand, the assurance of **resource optimization**, i.e. that "adequate and sufficient IT-related capabilities (people, process and technology) are available to support enterprise objectives effectively at optimal cost" (ISACA, 2012b, p. 43), is directly linked to the efficiency in management. In this sense, "the current

climate of cost reduction and budget restriction has resulted in new norm – there is an expectation that IT resources should always be used as efficiently as possible and that steps are taken to organize these IT resources ready for the next cycle of growth and new IT developments” (The National Computing Centre, 2005, p. 4).

Resources available to organizations comprise both human resources allocated for the execution of specific functions and financial resources available for investments in assets and services. In particular, human resources are considered to be among the main enablers of IT governance and management due to them being indispensable for structuring and delivering services. The degree of success of a governance strategy is directly related to the ability of the people within the organization.

Under the financial aspect, it is necessary to establish processes to manage the financial activities, covering IT budget, cost and benefits management, as well as the prioritization of expenditures in accordance with the adoption of formal budgeting practices and an organizational cost allocating system. Its goal is to foster a more effective and efficient use of IT resources, while also promoting transparency

and accountability on the cost and value of the demanded solutions and services. In summary, the goal is to enable the organization to make better decisions about the use of IT solutions and services, necessarily taking into consideration the costs and the available budget.

The establishment of a cost model based on the IT services definition ensures that the allocation of costs for services is identifiable, measurable and predictable, which encourages a more responsible use of resources, including those available through service providers. It is important to be able, through the management process, to compare actual costs with the budgets so that there is monitoring and reporting and, in case of deviations, these are identified in a timely fashion and have their impact assessed.

The process of **optimizing risk** levels, in turn, intends to “ensure that the enterprise’s risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of IT is identified and managed” (ISACA, 2012b, p. 39). In any organization, this approach favors the achievement of results, so that mitigation through appropriate controls has the potential to ensure greater effectiveness and efficiency from public

organizations. Depending on the situation of the evaluated sector, several measures can be adopted in order to institutionalize and improve risk management, as the implementation of a strategic planning process, active involvement of senior management with the implementation of risk management and investment in educational and training activities in this area.

In short, strengthening risk management in public organizations requires the improvement of internal controls, which, in turn, is a requirement for strong corporate governance. Thus, investing in risk management establishes an important foundation for governance.

Risk management, however, must be conducted interdependently with the delivery of benefits and the optimization of the use of resources, because these three factors collaborate with each other to deliver greater value to the organization.

This interconnection is visible when one realizes that the implementation of controls to mitigate risks, for example, consumes resources for its establishment and may have positive or even negative impacts on benefits delivery.

Although risks regarding information security are significantly connected to processes and resources related to IT, these are not the only kind of IT risk. There are several other types of risks that may affect the achievement of IT goals and objectives, such as: project risks; contracting risks; risks related to the availability of staff and/or funds; market, geopolitical, technological and regulatory risks, as well as other factors. For instance, the books “COBIT 5 for Risk” (ISACA, COBIT 5 for Risk, 2013c) and “Risk Scenarios – Using COBIT 5 for Risk” (ISACA, 2014, pp. 31-63) refer to a list of generic IT risks arranged in twenty different categories, showing that they go far beyond just the information security ones.

3. RISKS AND CONSEQUENCES

Some of the problems found in IT management of governmental organizations derive from the lack of proper IT governance. In this sense, it is possible to identify some common risks and their associated consequences.

3.1 Exposure to Information Security Risks

Due to inappropriate Information Security and Business Continuity Managements, many information security risks may arise from the absence of proper structures, processes and policies, such as:

- misappropriation of assets;
- unauthorized disclosure of information;
- unauthorized access;
- vulnerability to logical and physical attacks;
- information unavailability;

- misuse of information;
- noncompliance with personal data laws and regulations;
- failure to recover from disasters.

Thus, the IT security policy should state the organizational assets (data, equipment, business processes) that need protection and define procedures, tools and physical access controls in order to properly protect them.

Additionally, it is very important to define, organize, implement and execute a proper Business Continuity Management.

3.2 Deficiency in IT Planning

Failure to observe best practices in planning of IT can lead to:

- acquisitions of or spending in IT projects that are not priority;

- approval of IT projects that are not aligned with the organization's business needs;
- failure to meet targets set for the IT department;
- an IT department that does not adequately support other business areas.

3.3 Lack of an Implemented Software Process

The absence of implementation of a software process enables the occurrence of situations where purchased or developed software do not meet business needs and/or standards.

The following situations may occur:

- acquisition/development of software that does not meet the needs of the organization's business area;
- acquisition/development of software without quality check;
- development of software that is not implemented because it lacks standard quality;
- development of software that is incomplete or not in accordance with specifications;
- interruption or non-completion of software development projects.

4. ENABLERS OF IT GOVERNANCE

Enablers are factors that, individually or collectively, have the ability to influence the proper functioning of the organization's IT governance.

This guide will describe the seven categories of enablers described in COBIT 5, as well as how other relevant publications address the same concept.

4.1 Principles, Policies and Frameworks

According to COBIT 5, principles, policies and frameworks are the means by which governance decisions (direction setting) are institutionalized and, therefore, they act as integrating elements between these decisions and management, i.e. the execution of decisions (ISACA, 2012a, p. 31).

Principles express preferred behavior, set in order to guide decision-making and, as such, their implementation must be demanded by the leaders (ISO/IEC, 2008, 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

such as legality, impersonality, morality, publicity and efficiency.

In addition to principles, the use of guidelines is an important tool to direct the actions of IT management. They represent a set of more specific instructions or directions to achieve a certain goal and, together with the principles, define basic IT governance parameters for the organization.

As an illustration of such guidelines, the following could be given: the development of IT solutions must meet the standards established by the organization's IT sector; preliminary technical studies regarding the acquisition of IT solutions must necessarily consider the option for open source and free solutions; resources should be allocated primarily for the provision of the organization's strategic IT solutions; IT planning must rely on broad participation of business areas; and so on.

In order that the principles and guidelines be observed, it is necessary that these elements be properly transmitted throughout the organization. To achieve this, there should be policies in place that are clear and measurable, giving directions and driving desired behavior in order to condition the decisions taken within the

organization (ISO/IEC, 2008, p. 4). These policies, by providing a more detailed guidance on how to put principles into practice, end up influencing how decision-making aligns with the principles.

The governance framework, in turn, should provide structure, guidance and tools that enable the appropriate governance and management of IT. Indeed, the set of structuring mechanisms (principles, policies, processes, controls etc.) regarding IT governance that a particular institution intends to implement is that organization's specific governance framework.

Moreover, there are generic frameworks, such as the already mentioned COBIT 5 or the Information Technology Infrastructure Library (ITIL) that can support public organizations in the task of implementing processes and practices of IT governance, ultimately helping them in the process of building their own governance frameworks.

It is certain that every organization is free to define how their specific corporate framework will be structured. Nevertheless, they should analyze and articulate their IT governance requirements in order to put in place and maintain effective enabling structures, principles, policies,

guidelines, processes and practices, with clarity of responsibilities and enough authority to achieve the enterprise's mission, goals and objectives (ISACA, 2012b, p. 31).

With regard to IT governance, it is recommended that agencies and entities of the public administration establish at least one main policy that provides detailed guidance on how to put principles and guidelines into practice in order to guide the direction of IT within the institutional framework. This instrument is called IT Governance Policy (ITGP). For it to reach and be mandatory to all people in the organization, it must be formally approved by senior management, be easily, instantly and continually accessible to everyone and have its content widely spread and reinforced from time to time. It should also be required that the ITGP be periodically revised to suit the changes that occur in every organization over time.

In addition to establishing principles and guidelines, the ITGP should clarify who is responsible for each of the several activities related to IT governance in the organization, such as senior management, committees, IT managers and the IT and internal audit departments. Thus, it is expected that this policy sets, for example, who

is responsible for the preparation of IT plans, for monitoring the implementation of these plans, for overseeing and monitoring IT performance, for assessing IT risks that may have impact on the organization's business, among other responsibilities. Put another way, the ITGP should clearly establish the roles and responsibilities of each stakeholder in the governance of IT.

4.2 Processes

In the context of governance and IT management, the term process is used to describe an organized set of practices and activities to achieve certain goals and produce a set of outputs in order to support the achievement of IT goals of an organization (ISACA, 2012a, p. 27).

COBIT 5 establishes a set of 37 processes, five of which are related to IT governance and 32 linked to the management of IT processes. IT governance processes deal with processes associated with delivering value and optimization of risk and resource objectives, and include practices and activities directed to the evaluation of strategic options, providing direction and monitoring of results. In turn, management processes include responsibilities related to planning,

implementation, execution and monitoring of the activities performed by the IT industry organization (ISACA, 2012b, pp. 23-24).

In public administration, there is not a unique set of processes and practices that must be implemented by all organizations, because of the diversity of institutions. Organization's strategic importance to the state, size of the institution, industry expertise, resources and funding available for investment in IT, IT goals and business maturity in IT governance, level of acceptable risks etc., are all factors that influence the ability to implement processes. Thus, it is reasonable to expect that organizations that are larger, more complex and more dependent on IT plan to implement more processes and practices than smaller and simpler institutions. However, regardless of the number of processes, all of them should be able to properly govern and manage their own IT in accordance with their goals and needs.

Considering this, every public organization should take into account their own specific situation to select the processes of governance and management of IT they will implement. As a consequence, it is not recommended that every public institution deploy and manage with the same degree of depth all 37 processes and 210

practices defined within the COBIT 5, for example, since they would be at risk of wasting resources deploying processes that may not generate clear benefits to the organization.

4.3 Organizational Structures

Organizational structures play a key role in decision-making in any organization. They are composed of stakeholders, each with their own roles and interests. Levels of authority for these structures, defined for decision-making and other activities they perform, are established by organizational policies, such as the ITGP.

The decisions taken within the organization that guide the actions of management and IT are critical for good IT governance. Important issues related to resource allocation or to investment and prioritization of IT projects are typically decided by organizational structures, such as the senior management and the IT committee. Other governance structures, such as the IT department, the internal audit department, the area responsible for risk management (corporate or IT) and the office of IT projects play an important role in producing information that will be used by the final decision-makers.

To operate properly, it is recommended to define a set of rules that describes the *modus operandi* of each structure. For example, the definition of its mandate and competencies, responsibilities of each role contained in the structure, the possibility of delegation of powers, the frequency of meetings, and the situations in which the decision must be escalated to a higher authority. For these rules to be observed within the public administration, it is recommended that they be consolidated in a single formal document that describes the organization and operation of these structures, such as by laws.

There are several organizational structures that relate and enable governance and IT management in an institution, and their relations, in order to reflect business needs and IT priorities. This is the object of management practice APO01.01 - Define the organizational structure (ISACA, 2012b, p. 52). The choice of which structures will be adopted is the responsibility of each organization, depending on its context, available resources and needs.

In any case, whatever the organizational structures chosen by the institution, it is necessary that top management ensure the allocation of the necessary resources (both human and financial)

to the components of these structures for them to perform their duties adequately. Otherwise, there is the risk that organizational structures are only formally defined, but do not have their members effectively meeting and deliberating on governance and IT management issues.

4.4 Culture, Ethics and Behavior

The implementation and improvement of IT governance institutions depend on the application of good practices related to the theme, however it is still not enough if the only transformations are of technological nature. It is necessary that people, whether members of senior management, managers or belonging to operational IT sectors, be committed to the changes implemented through the adoption of new policies, processes and practices related to the management and use of IT. Thus, one can say that the human component is a critical success factor for IT governance.

Indeed, culture, ethics, and behavior relate to the set of individual and collective behaviors in an organization, and should be taken into consideration in the formulation of the principles that will drive the use and management

of IT. These principles are usually communicated through corporate policies, which can also come to establish the consequences resulting from non-compliance with the expected ethical conduct.

This enabler is an important aspect of IT governance so that other mechanisms can adequately fulfill their functions. IT processes, although well defined, may not achieve the expected results if the stakeholders are not effectively engaged in performing process activities as they were planned. Likewise, the effectiveness of organizational structures on improving the governance and management of IT depends on the proper implementation of the decisions they make, which cannot occur if people in charge are not sufficiently motivated or committed to the organization.

To illustrate how cultural aspects influence IT governance in an institution, it is possible to mention some examples: IT committees not deliberating on strategic issues of IT, because their members are more interested in power struggles and end up discussing issues of little relevance; influential people in the organization effectively determine the prioritization of IT projects without following the

previously defined criteria for prioritization; senior management who do not monitor IT's performance indicators and do not make decisions concerning IT, considering that IT concerns exclusively to the IT department, not to them.

Therefore, it is understood that efforts related to the governance and management of IT cannot be effective if people's involvement is not deep enough to bring about the required changes. It is necessary that senior management set the expected behaviors and track their adoption by the rest of the organization.

Accordingly, campaigns should be adopted to raise awareness, such as workshops and training for the people responsible for making decisions and for enforcing compliance with policies, plans and practices. IT professionals have the understanding that engagement of everyone in improving the governance of IT in the organization is an essential component for achieving the business objectives and thus to fulfill the institutional mission. In COBIT 5, the fourth activity within the management practice APO07.03 - Maintain the skills and competencies of personnel - recommends the improvement of behavior skills as part of the

training activities of staff within the organization (ISACA, 2012b, p. 85).

Another good practice related to the cultural component consists of leaders responsible for IT governance adopting the behavior to be followed by others in the organization, thus exerting leadership by example. This is an effective way to convey the values and principles of governance established in the corporate policies (e.g. ITGP and code of ethics).

4.5 People, Skills and Competencies

People are the most important asset of an organization. They are the ones that, by using their skills and expertise, perform a set of activities that aim to meet the business needs, in order to comply with the institutional mission.

With regard to IT governance, people, skills and competencies are required for correct decision-making. To achieve roles that are properly performed within organizational structures as well as for the processes of governance and management of IT to be run successfully, it is necessary that the people involved be

adequately qualified, equipped with the technical and behavioral skills required for the work.

Therefore, it is important that public institutions conduct the management of their human resources in order to make sure that those responsible for the actions of governance and IT management are committed and sufficiently skilled to perform their functions. On this subject, COBIT 5 defines the process APO07 - Manage Human Resources, related to the maintenance of appropriate personnel, planning and monitoring of the use of IT human resources and business activities, among others (ISACA, 2012b, pp. 83-84).

In this context, it is recommended that the agencies and entities of the public administration periodically survey the skills and competencies needed to perform the attributions of the personnel, including those not related to IT. Based on this survey, it is possible to plan the strategy for obtaining the knowledge that the institution is in lack of, whether through training actions or by recruitment.

Besides the aspect of professional qualification, public institutions need to have personnel in quantities compatible with the implementation of actions related to the governance

and management of IT in the organization. Therefore, it is necessary to carry out preliminary studies that can support any internal redeployment of staff to allocate these functions or even justify hiring outside personnel.

4.6 Information

Information is pervasive throughout any organization and includes all information produced and used by the enterprise (ISACA, 2012a, p. 27). Information is the key element that connects all people, business processes, organizational units and everything needed in the process of value creation inside and outside an organization.

According to the Taking Governance Forward view, information is an enabler for enterprise governance. Governance needs to ensure not only information is available to the enterprise but also for the governance body itself. Thus, a governance system must have as a primary concern to establish proper information flow throughout the organization.

In the information cycle, business processes generate and process data, transforming them into information and knowledge, and

ultimately generating value for the enterprise (ISACA, 2012a, p. 81).

Information is used at both management and governance levels. Managers must monitor using measurement systems properly, as well as need to receive information to fulfill their responsibilities and commitments (ISO/IEC, 2008, pp. 8-9). Governance uses information for evaluating, directing and monitoring the enterprise.

Hence, it is recommended that agencies and public organizations establish robust information systems to provide effective information to their stakeholders. COBIT 5 means effective as in the appropriate amount, relevant, understandable, interpretable and objective. Other criteria as efficiency, integrity, reliability, availability, confidentiality and compliance must also be considered as governance goals related to information.

4.7 Services, Infrastructure and Applications

Services, infrastructure and applications include the technology that provide the enterprise with the capability to process the information required to run the business. At the very

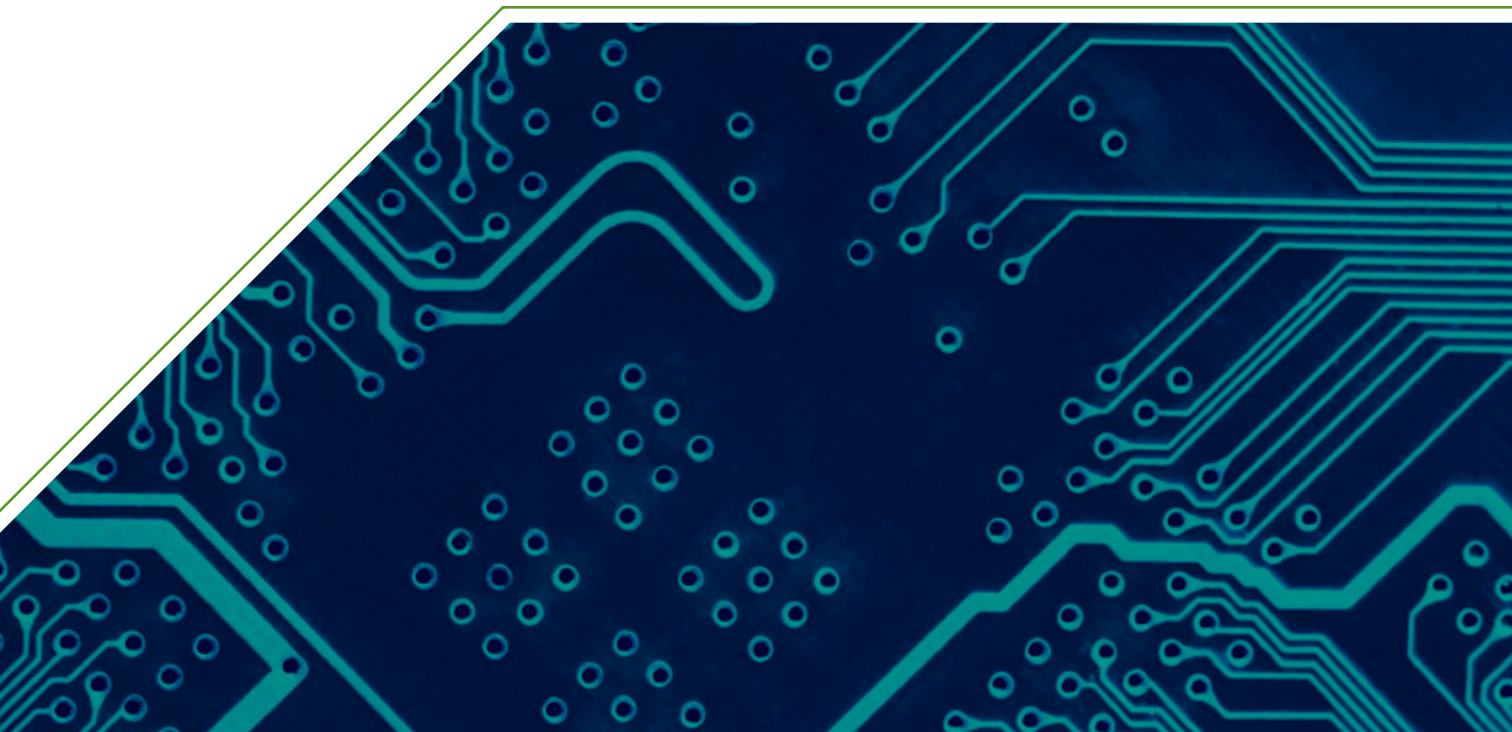
end, these technical elements are the building blocks in which an IT organization relies on to deliver value to the enterprise.

Thus, inadequate IT systems may expose organizations to unwanted risks and negatively influence business performance. In the other hand, good IT services improve business capabilities as well as enable exploration of new opportunities.

In terms of governance, services are required, supported by applications and infrastructure

to provide the governance body with adequate information and to support the governance activities of evaluating, setting direction and monitoring (ISACA, 2012a, p. 31).

A definition of an enterprise architecture that include business processes, information models, applications and infrastructure is essential to any organization. IT governance must take into consideration the most appropriate architecture viewpoints to meet the needs of different stakeholders (ISACA, 2012a, p. 86).



GOVERNANCE EVALUATION TECHNIQUES FOR IT (GET.IT)

Chapter

02



W

ithout 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.

1. AUDITING INDIVIDUAL ORGANIZATIONS

1.1 Introduction

In today's environment, organizations are practically unable to accomplish their mission without utilizing IT. Furthermore, there is an increasing demand to a more efficient use of the limited revenue that organizations have to manage their business operations. Salary and fixed costs, such as rent, equipment etc., make increasing demands on limited resources.

Thus, IT resources are constantly competing with other requirements, making the case for an ever more efficient and focused use of the resources allocated for IT. In this sense, good IT governance can go a long way in ensuring that appropriate value is gained from the existing and future IT infrastructure, processes and other resources.

1.2 Role of the IT Auditor

The role of the IT auditor, when looking at IT governance in an organization with a focus on projects, is to understand the management

framework in place. He should ask questions like: Are projects selected, controlled and evaluated in an effective and comprehensive way to warrant business goals are met ? Additionally, does the framework impose periodic analysis and revision of the controls?

Additionally, his role in providing assurance to management regarding IT issues is also very important. Technical concerns that cannot be verified by management, like business continuity, operational costs, IT investments' ROIs, quality and reliability are common topics of interest. Ensuring that IT is aligned to the business needs and investigating IT risks on the business are also major activities that can be carried out by the IT auditor.

1.3 Internal Control

Internal control is the process of introducing and implementing a system of measures and procedures to determine whether the organization's activities are and remain consistent with the

approved plans and contribute to the overall objectives of the organization. If required, necessary corrective measures are taken so that the policy objectives can be achieved. Internal control keeps the IT system on course. Internal controls include risk management, compliance with internal procedures and instructions and with external legislation and regulations, periodic and ad hoc management reports, progress checks and revision of plans and audits, evaluations and monitoring.

1.3.1 Risk Management

The management of IT risks should form an integral part of the company's risk management strategy and policies. Risk management involves identification of risks concerning existing applications and IT infrastructures, and continuous management, including an annual / periodic review and update by the management of the risks and monitoring of mitigation strategies.

1.3.2 Compliance Mechanism

Organizations need to have a compliance mechanism that ensures that all the policies and associated procedures are being followed. Basically, it is the organization's culture which makes all the employees sensitive about all non-compliance issues.

The compliance supporting mechanism may also include the quality assurance group, security staff, automated tools, etc. A report of non-compliance should be reviewed by appropriate management and serious or repeated non-compliance issues must be dealt with. Management may choose to deal with non-compliance with refresher training, modified procedures, or even an escalating retribution procedure depending on the nature of the non-compliance (security violations, missing mandatory training etc.).

Independent assurance, in the form of internal or external audits (or reviews) can provide timely feedback about compliance of IT with the organization's policies, standards, procedures, and overall objectives. These audits must be performed in an unbiased and objective manner, so that the managers are provided with a fair assessment of the IT project being audited.

1.4 Investment Decisions (Development / Acquisition of Solutions)

IT governance should provide business users with solutions to their new or modified requirements. These can be accomplished by the IT department

through either developing (building) new software or systems or acquiring these from vendors on a cost-effective basis. In order to achieve these successfully, best practices typically require a disciplined approach where requirements are identified, analyzed, prioritized and approved, a cost-benefit analysis conducted among competing solutions and the optimum solution selected (for example, one which balances cost and risk).

1.5 IT Operations

IT operations is typically the day-to-day running of the IT infrastructure to support business needs. Properly managed IT operations make it possible to identify bottlenecks and plan for anticipated capacity changes (additional hardware, or network resources), measures performance to ensure it meets the agreed-upon needs of the business owners, and provides help desk and incident management support to the users of IT resources.

1.6 People and Resources

It is recommended that management ensure through regular assessments that sufficient

resources are allocated to IT for meeting the needs of the organization, according to agreed priorities and budget constraints. Furthermore, the human aspect should be respected by the policies, practices and IT decisions, which should consider the current and future needs of process participants. Governance management should regularly assess whether or not resources are being used and prioritized as the business objectives demand.

1.7 Planning IT Governance with Success in Mind

Since IT governance is a continuous process, planning is a very important step to make it succeed. During planning, many factors are major contributors to its success and, as such, should be closely watched:

- Control requirements need to be coordinated between the IT and the business in order to assure that approaching governance is comprehensive of the whole organization. It is beneficial to have a committee in place to set, agree and monitor the directions and policies. While IT needs to adapt a model that applies on all of its units. It is very important

that the scope of IT governance is communicated and approved by top management;

- Both the business and the IT in the organization need to define and agree on the base for responsibilities and accountabilities. IT governance needs the commitment of the high management and this will also need a high level direction to mandate the organization;
- Due to the complexity of IT governance, a clear and comprehensive framework needs to be developed or adopted. The framework needs to include all IT processes and their respective controls. Additionally, to make IT governance more relevant, it needs to be linked to the corporate governance;
- IT governance needs to be promoted in the organization by means of awareness campaigns and clear communications. Incentives to complying with IT governance is also a possible way to motivate a positive culture in the organization;
- Work to promote the IT function of the organization as a familiar trusted professional service provider. This helps to better integrate IT and business to promote more trust;
- Create an IT performance measurement framework/process in order to monitor the success of goals, objectives and projects;
- Monitor financial gains or savings that result from the implementation of IT governance. This will help get more support from management for other related initiatives;
- It is likely that there will be opportunities to make financial savings as a consequence of implementing improved IT governance. These will help to gain support for improvement initiatives.

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 risks. Luckily, for us, the risks are effectively managed if the key elements of IT governance are in place. Thus, we will focus our audit objectives on the key elements and create a line of audit or question to satisfy us of their approach to IT governance.

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

Assess whether the organization's leadership effectively directs, evaluates and monitors IT use in the organization in order to fulfill the organization's mission.

Related Audit Issues:

- **Defining IT requirements:** How does the organization identify and approve business and IT requirements?
- **Leadership:** How does the leadership direct and monitor the performance of business and IT objectives on a periodic basis?
- **IT investments:** How does the organization manage IT investments?

1.8.2 Audit Objective (2) IT Strategy

Confirm whether there is an IT strategy in place, including an IT plan and the processes for the strategy's development, approval, implementation and maintenance, which are aligned with the organization's strategies

and objectives. The risks and resources while accomplishing IT objectives are effectively managed.

Related Audit Issues:

- **Quality of IT strategy:** Does the organization have an IT Strategy that serves to guide its IT functions?
- **Risk management:** How does the organization manage its risks?

1.8.3 Audit Objective (3) Organizational Structures, Policy and Procedures

Ensure that there are organizational structures, policy, and procedures in place that enable the organization to meet its mandate for business goals.

Related Audit Issues:

- **Organizational structures:** Does the structure of the IT Organization enable it to meet its IT Goals and business needs?
- **Policy and procedures:** Has the organization approved and is it using appropriate

policies and procedures to guide its business and IT operations?

1.8.4 Audit Objective (4) People and Resources

To assess whether sufficiently qualified/trained personnel are employed and that they have access to suitable resources that enable the organization to meet its business goals.

Related Audit Issues:

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

1.8.5 Audit Objective (5) Risk Assessment and Compliance Mechanisms

To assess whether the organization has a risk assessment and compliance mechanism that enable them to take corrective action as necessary.

Related Audit Issues:

- **Risk Assessment:** How does the organization identify, prioritize, and manage risks with respect to IT?

- **Compliance mechanism:** How does the organization ensure that it has an adequate and working compliance mechanism to ensure all policies and procedures are being followed?

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 resource constraints and must strive to ensure that IT resources are effectively identified, managed and utilized. Since this is a smaller organization, many of the policies may be missing and personnel may not be aware of operating procedures in group meetings or emails. Furthermore, since the IT group is relatively small, individuals might be responsible for more than one function (security and risk officer, for example) and thus they may not be organized in a manner that the auditor is generally expecting. The audit objectives listed below are just one example of how the auditor can tailor the audit to a smaller entity.

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

Assess whether the organization's leadership effectively directs, evaluates and monitors IT use in the organization in order to fulfill the organization's mission.

Related Audit Issues:

- **Defining IT requirements:** Apart from the IT Group, who in the organization is involved in identifying business and IT requirements?
- **Leadership:** Whom does the IT group report to as it implements and operates the IT environment?
- **IT investments:** Is the IT group able to justify its IT expenditures and resources?

1.9.2 Audit Objective (2) IT Strategy

Confirm whether there is an IT strategy in place, including an IT plan and the processes for the strategy's development, approval, implementation and maintenance, which is aligned with the organization's strategies

and objectives. The risks and resources while accomplishing IT objectives are effectively managed.

Related Audit Issues:

- **IT strategy:** What is the overall vision of the IT group as it operates the IT infrastructure?
- **Future:** Is the IT group aware of what the business users want from them in the next two years?

1.9.3 Audit Objective (3) Organizational Structures, Policy and Procedures

Ensure that there are organizational structures, policy, and procedures in place that enable the organization to meet its mandate for business goals.

Related Audit Issues:

- **Organizational structures:** Are members of the IT group aware of their roles and responsibilities with respect to IT? Are the business users aware of whom to contact in the IT department on issues related to security, operations, new functionality etc.?

- **Policy and procedures:** How does the IT group disseminate new information to the business users? How do they ensure that their own internal (IT Personnel) are aware of the new procedures or guidelines with respect to IT?

1.9.4 Audit Objective (4) People and Resources

To assess whether sufficiently qualified/trained personnel are employed and that they have access to suitable resources that enable the organization to meet its business goals.

Related Audit Issues:

- **HR and logistics:** Are personnel in the IT group sufficiently qualified, periodically trained, and updated regarding new or emerging IT issues?

1.9.5 Audit Objective (5) Risk Assessment and Compliance Mechanisms

To assess whether the organization has a risk assessment and compliance mechanism that enable them to take corrective action as necessary.

Related Audit Issues:

- **Risk assessment:** What risk assessments has the IT group conducted and what actions have been taken as a result?

1.10 IT governance and Performance Measurement

There is no doubt that a practical and effective way to measure IT performance is an essential part of any IT governance program, just as transparency and reliability of financial results is a corporate governance necessity. Performance management is important because it verifies the achievement of strategic IT objectives and provides for a review of IT performance and the contribution of IT to the business (i.e. delivery of promised business value). It is also important in providing a transparent assessment of IT's capability and an early warning system for risks and pitfalls that might otherwise have been missed. Performance measurement provides transparency of IT related costs, which increasingly account for a very significant proportion of most organizations' operating expenses.

The value of good IT systems is that they can improve the economy, efficiency and effectiveness of existing programs and contribute to better public services. IT systems can be an efficient and effective program delivery mechanism. They have the potential to deliver existing services at reduced cost and to provide a range of additional services, including program performance information, with greater efficiency, security, and control than is available in manual systems. However, IT systems also have the potential to result in major systemic errors with a resultant greater impact on agency performance than would be possible if manual systems are used.

The approach to performance auditing in an IT environment should involve the following inter-related processes:

- obtain an understanding of the auditees' IT systems and determine their significance for the performance audit objective;
 - identify the extent of IT systems auditing required to achieve the performance audit objective (e.g. audit of IT-investment processes and their links to business strategies, audit of systems development; audit of environment and applications controls) and employ specialist information system/IT auditors to undertake the task; and
 - develop and use, when appropriate, computer-assisted audit techniques to facilitate the audit.
- A performance audit in an IT environment should:
- assess whether the IT systems enhance the economy, efficiency, and effectiveness of the program's objectives and its management, especially in relation to program planning, execution, monitoring, and feedback;
 - determine whether system outputs meet established quality, service and cost delivery parameters;
 - identify any deficiencies in information systems and IT controls and the resultant effect on the efficiency, economy, and effectiveness of performance;
 - compare the IT system development and maintenance practices of the auditee to leading practices and standards; and

- compare the IT strategic planning, risk management, and project management practices of the auditee to leading practices and standards including corporate governance practices.

1.11 Performance Aspects of Auditing in an IT Environment

In many cases, the most important issue of the audit is to establish whether the IT system has enhanced the efficiency with which the auditee manages its programs and whether the IT system has beneficial results for the stakeholders.

The auditor may also be expected to assess if the IT systems have facilitated improved program management. Some areas to be considered include:

- The IT investment process: especially the auditee's innovation system for creating, processing and deciding on IT investment proposals – linkage to business strategy, management and planning processes;
- IT should support the objectives and business strategy of the auditee and, therefore, is an integral part of its operations;

- IT operations require highly qualified staff;
- The contribution of IT to operations is measured in operational efficiency terms;
- The benefits of IT may not be realized without appropriate changes;
- Normal value for money measures may be more difficult to apply. In addition to assessing whether the auditee's IT systems represent value for money, the performance auditor may also be expected to measure if the IT environment has contributed to transparency, accountability, and good governance.

The audit may also contain IT issues that are more specialized, i.e. IT system development and operational management.

1.12 Performance Auditing Involving IT System Development

A performance audit involving IT systems development should determine if the audited entity:

- has the appropriate executive approval for the development of the IT system, i.e., that

IT management fits in the corporate governance of the auditee;

- has appropriate project management processes in place to manage the project;
- has met required targets of time, cost, system function, and value for money;
- uses an appropriate system development methodology; and
- has processes in place, including the involvement of internal auditors, to ensure that the new system includes all the necessary controls and audit trails, and is likely to meet the requirements of the auditee and its stakeholders.

1.13 Performance Auditing Involving Operational IT Systems

The following list contains some of the more important concerns that the auditor would be expected to consider and should be modified as required for the specific entity being audited:

- the strategic and operational management of IT, including assurance that IT is included

in the overall corporate governance of the auditee;

- risk management practices in relation to IT;
- IT system design, development, and maintenance controls;
- compliance with standards, including external standards;
- application controls;
- processing controls, including audit trails;
- business continuity arrangements;
- data integrity, including sampling of data (possibly using computer-assisted audit techniques);
- access controls and the physical and logical security of networks and computers, including Internet firewalls;
- controls as a safeguard against illegal software;
- performance management and measurement; and

- other issues that arise during the audit.

In making the assessment the auditor may:

- review files and other documents relevant to the development and operation of the IT systems;
- interview the Auditor General and key staff members;
- use an appropriate software package to test the central and networked computing system controls; and
- test a sample of transactions (potential for using computer-assisted audit techniques) to validate the systems and relevant controls.



2. STATE-LEVEL / PERFORMANCE AUDITING

2.1 Introduction

Supreme Audit Institutions (SAIs) audit the activities of the government, its administrative authorities and other subordinate institutions. SAIs form part of an overall legal and constitutional system within their respective countries, and are accountable to various parties, including legislative bodies and the public. SAIs are also responsible for planning and conducting the scope of their work and using proper methodologies and standards to ensure that they promote accountability and transparency over public activities, meet their legal mandate and fulfil their responsibilities in a complete and objective manner. The concept of accountability refers to the legal and reporting framework, organizational structure, strategy, procedures and actions to help ensure that SAIs report on the regularity and the efficiency of the use of public funds to the legislative body (Parliament). As the Lima Declaration states “SAI shall be empowered and required by the Constitution to report its findings annually and independently to Parliament or any other responsible public body”.

For the purpose of this chapter, the terms state-level auditing and performance auditing will refer to the same concept. According to the guidance provided by INTOSAI performance auditing is mainly concerned with the economy, efficiency and effectiveness of government programs.

Moreover, SAIs may carry out audits or other engagements on any subject of relevance to the responsibilities of management and those charged with governance and the appropriate use of public resources. These engagements may include reporting on the internal control standards. In the case of the extensive use of information systems in all public organizations, information technology (IT) controls have become increasingly important.

Furthermore, to serve as a credible voice for beneficial change, it is important that SAIs have a good understanding of developments in the wider public sector and undertake a meaningful dialogue with stakeholders about how the SAI's work can facilitate improvement in the public

sector. Consequently, IS performance auditing may be started on the grounds of audit results of IS general controls and application controls. Special report on internal controls in public sector also can be prepared to the legislative body (Parliament). Those reports usually includes chapters on IT controls in the public sector.

The important point to consider when conducting state-level / performance audits is the assurance professional's ability to gather adequate knowledge about how government / state machinery works. This is critical when planning to assess any government program.

2.2 State-level IT Assurance Framework

As the Lima Declaration states “Audit is not an end in itself but an indispensable part of a regulatory system whose aim is to reveal deviations from accepted standards and violations of the principles of legality, efficiency, effectiveness and economy of financial management early enough to make it possible to take corrective action in individual cases, to make those accountable accept responsibility, to obtain compensation, or to take steps to

prevent--or at least render more difficult--such breaches”. Hence, any audit should be a part of wider assurance framework.

As described in COBIT 5 for Assurance (ISACA, 2013d), an important component of IT assurance framework is three-party relationship involving an accountable party for the subject matter, an assurance professional and an intended user:

- An accountable party is the individual, group or entity (auditee), usually involving management, that is ultimately responsible for subject matter, process or scope. An assurance engagement involves two other parties;
- Depending on the circumstances, the user could include a variety of stakeholders, such as shareholders, creditors, customers, the board of directors, the audit committee, legislators or regulators. For some types of assurance activities, the auditee and the user can be identical, e.g., IT management;
- The assurance professional (auditor) is the person who has overall responsibility for the performance of the assurance engagement and for the issuance of the report on the subject matter.

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.

The processes comprised in the Monitor, Evaluate and Assess (MEA) domain of COBIT 5 can be regarded as the core assurance processes. More specifically, the MEA02 process is dedicated to monitoring, evaluation and assessment of internal control.

2.3 Public Sector's Perspective of IT Governance

Matters of corporate governance are shared among the board, senior management and the audit function. Worldwide, public sector organizations employ a variety of governance

structures that are based on the underlying principles of accountability and transparency. The role of IT governance as a means of demonstrating these principles in terms of government investment in IT should be investigated with the aim of ensuring effective e-governance and service delivery. As IT governance does not function separately from the corporate governance processes of an organization, a credible and effective governance system has to take the relationships among the participants in the process into account. Within the context of the public sector, the role of the board of directors / executive authority, senior management and the audit function can be briefly explained as follows.

2.3.1 Board of Directors / Executive Authority

The responsibility of the board of directors / executive authority is to oversee and direct the management of the organization. This is the highest level of an organization's decision-making structure. Their commitment to the fostering of good governance principles in the organization ensures ethical behavior and a culture of compliance with the rules and regulations of the organization.

2.3.2 Senior / Executive Management

Senior / executive managers play a critical role in ensuring that their organization's IT governance system and related processes are effective and demonstrate the ethics of the organization and a culture of compliance with business and IT processes. Management thus sets an example that employees can emulate in the way they act and do their work. The International Auditing Standards refer to this level of management as “those that are charged with governance”.

2.3.3 Audit Function

According to Richard Brisebois, Greg Boyd and Ziad Shadid from SAI Canada, the role of the IS auditor with regard to IT governance is described as follows (Brisebois, Boyd & Shadid):

- To provide assurance and recommendations with regard to the establishment of effective IT governance performance metrics;
- To promote and elevate the need for IT governance and the establishment of processes to the highest decision-making level in an organization;

- To play an advocacy role in promoting various IT governance strategies to ensure that management is informed about the problems, risks and rewards that arise from the use of IT.

In the WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions, IT governance is described as follows (INTOSAI, 2014):

...the overall framework that guides IT operations in an organization to ensure that it meets the needs of the business today and that it incorporates plans for future needs and growth. It is also an integral part of the enterprise governance, and comprises the organizational leadership, institutional structures and processes, and other mechanisms (i.e. reporting & feedback, enforcement, resources etc.) that ensure that IT systems sustain organizational goals and strategy while balancing risks and effectively managing resources.

2.4 IT Governance Assessment Process

As mentioned above, IT governance assessment process at state level can be done in three steps:

2.4.1 Evaluation of Public Entities Internal Control

Is auditors perform their own proprietary evaluations of IT internal control at institutional level. In such cases not only legal compliance is examined, but specific to institution audit approach is used which is based on risk assessment, when the critical IT processes are selected and further examined and evaluated against standards and the best practices. IT maturity levels are examined, recommendations are made for IT internal control improvements that are already beyond legislative compliance. As an example, one further step may be suggested in COBIT maturity scheme in selected IT processes, therefore actions to be done to achieve this. Such audits provide IS auditors with in-depth knowledge on current status of IT governance at institutional level. Added value – possibility to find similar problems in similar institutions and possible indication to the auditor that the cause of the problems is not within the audited institution. In most cases, recommendations of such IT audits are provided to the audited ministry or agency.

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

Those audits are used to give an audit opinion on the most important IT issues. Audits are complex, aimed at program level when a program is managed by several ministries or agencies, thus requiring conformity of institutional strategies and coordination of actions in addition to their own IT matters. This gives another dimension of information to IS auditor – the possible weaknesses of strategic alignment and practical inter-ministerial coordination. Findings are measured against standards and best practices. As the reasons for weaknesses in most cases are beyond a single ministry or agency, recommendations in such cases go to the Government (or the Prime Ministers Office).

Assurance professionals should be aware of the intricacies that come with the implementation of government programs or interventions and the impact they have in their areas of responsibilities. The adoption of an IT governance framework therefore requires that an assessment strategy or approach be established that is flexible enough to provide

assurance and highlight the extent to which governance processes are addressing government's service delivery objectives. Typically, the following questions are critical when conducting state-level / performance audits of the IT governance processes:

- Is there a clear structure of performance goals and have the appropriate priorities and instruments been chosen for the use of public funds?
- Is there a clear distribution of responsibility between the different levels of authority, bearing in mind the principle of subsidiarity?
- Is there general awareness of cost and an orientation towards the rendering of services, putting citizens' needs in focus?
- Is there an adequate emphasis on management controls and reporting requirements?

2.4.3 Auditing IT Internal Control at the Governmental Level

Information obtained during IT internal control audits and IT 3E audits gives possibility

to measure effectiveness of IT internal control at the governmental level, looking at different ministries/agencies (and coordination of strategic initiatives as well as implementation of trans-ministerial programs) like SAIs look at structural units of a traditional organization with their own functions and responsibilities. Recommendations of such audits normally go to the Government (or the Prime Ministers Office), sometimes asking Government for further actions which is beyond direct competence of the Government. After major primary legal acts are adopted by the Parliament, practical enforcement has to be assured by the Government by issuing secondary legislation to support the main (or primary) legal act. Based on knowledge on readiness of the public sector to be placed in the new legislative environment, SAI can suggest some positives from standards/ the best practices which are needed for public sector and which are not so difficult to implement. Then again: after new legislation is enforced, SAI should look at ministries/agencies one again are they successful to act in the new legislative framework and if it appears that mistakes are caused by possibly non-adequate legislative framework, SAI should be here once again to suggest measures for its improvement.

2.5 State-level / Performance Audit Considerations

The INTOSAI Code of Ethics and Auditing Standards as well as the relevant SAI standards and guidelines applicable to performance auditing should always be followed when conducting state-level / performance audits. Prior to engaging in a performance audit, the auditor must have a well-defined scope and plan to guide the audit process.

2.5.1 Objective

State-level / performance audits are conducted to determine whether government interventions, programs and institutions are performing in accordance with the principles of economy, efficiency and effectiveness and whether there is room for improvement. They provide clients with information and assurance about the quality of the management of public resources and they also assist public sector managers by identifying and promoting better management practices.

2.6 State-level / IT Internal Control Audit Considerations

2.6.1 IT Internal Control Audit Considerations

Information technology controls relate to each of the components of an entity's internal control process including the control environment, risk assessment, control activities, information and communication, as well as monitoring. Those five domains are incorporated in the famous COSO framework.

COSO's Internal Control–Integrated Framework and Enterprise Risk Management–Integrated Framework are frequently referenced sources of information. However, those frameworks are not focused on IT. COSO-based control environment should be augmented with IT control objectives more detailed to assess the IT control environment effectively.

A widely used IT governance and control framework is the ISACA Control Objectives for Information and Related Technology (COBIT), which was originally published in 1994. The 5th version of COBIT was released in 2012. COBIT is not intended to compete with COSO or other

frameworks, but it can be used to complement them by augmenting the others with more robust IT-specific control objectives. COBIT offers a generally accepted set of IT control objectives (process practices and process activities since COBIT 5) that helps management to conceptualize an approach for measuring and managing it risk. COBIT 5 is generic and useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector, therefore it can be used by big public systems (a government is the system by which a state or community is governed). Moreover, the organization does not have to be currently using COBIT 5 to use COBIT 5 for Assurance (ISACA, 2013d).

2.6.2 State-level IT Internal Control Audit Considerations

As “government” is occasionally used in English as a synonym for “governance”, the core activities of the government, related to IT governance, are in the Evaluate, Direct and Monitor (EDM) domain of COBIT 5. This domain contains five governance processes:

- EDM01 Ensure Governance Framework Setting and Maintenance;
- EDM02 Ensure Benefits Delivery;

- EDM03 Ensure Risk Optimisation;
- EDM04 Ensure Resource Optimisation;
- EDM05 Ensure Stakeholder Transparency.

Auditors can use the set of audit/assurance programs based on COBIT 5 for conducting assurance over a governance process. The programs are aligned with generally accepted auditing standards and practices and are based upon the overall assurance engagement approach, which is divided into three phases:

- **Phase A:** Determining the scope of the assurance initiative;
- **Phase B:** Understanding enablers, setting suitable assessment criteria and performing the assessment;
- **Phase C:** Communicating and reporting the results of the assessment.

ISACA has developed examples of Audit/Assurance programs for all COBIT 5 EDM processes, which may be found on the ISACA Knowledge Center (ISACA, Audit/Assurance Programs).

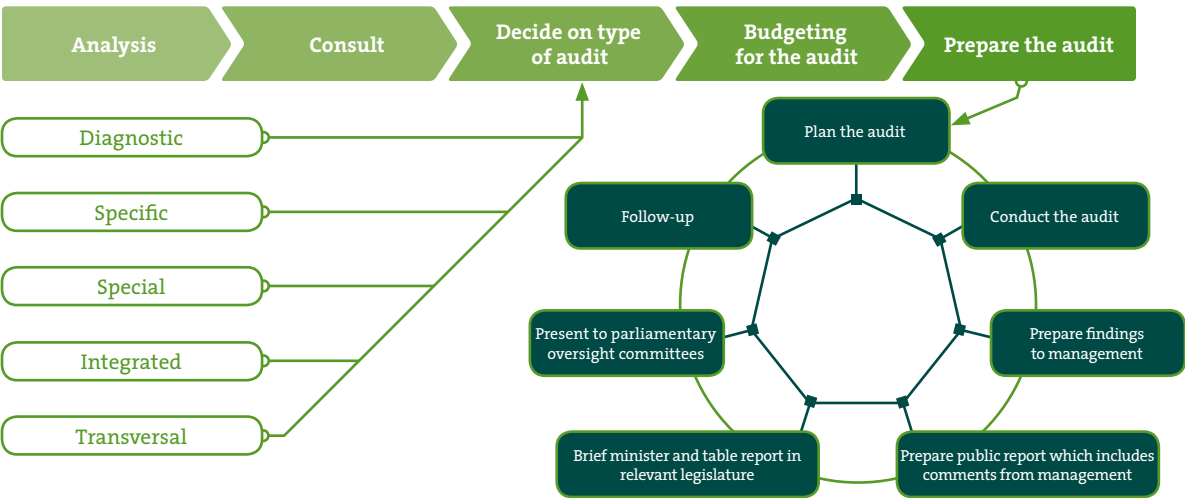
In practice, assurance professionals will have to use their own professional judgment when developing their own customized audit programs, to avoid duplication of work.

2.7 State-level Audit Process

Before initiating the processes depicted in the diagram below, the following steps provide a good starting point in obtaining the necessary understanding of the environment/organization to be assessed:

- Gather governance documents outlining the structures and functions of government regarding the planning, management and monitoring of government investment in IT;
- Review governance processes and structures at the organization or department to gain perspective about their functioning;
- Establish assessment criteria and a maturity level for the state of IT governance processes across government.

Figure 3: Performance audit process



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.

Consultation with the subject matter specialist is paramount and will ensure that the audit is correctly focused and that all stakeholders are clear about the objective and expected results. The outcome of the analysis and consultation stages provides auditors with enough information to decide on the type of audit to conduct to provide an independent, objective and reliable examination of whether government programs, systems, activities or organizations provide value for money in the services they render to citizens.

The following types of audit can be performed, depending on the objective or the type of assurance that the auditor wants to provide to the stakeholders:

- **Diagnostic:** a short audit using tools such as questionnaires or web-based surveys;

- **Specific:** a short audit that answers specific questions about an entity or program;
- **Special:** a joint audit that combines the various audit disciplines and expertise in the SAI;
- **Integrated:** performance audit procedures are carried out during the annual financial audits;
- **Transversal:** an audit that focuses on cross-cutting issues.

When a decision has been made on the type of audit to be conducted, it can be assumed, without getting into details, that important activities of the audit process have been taken care of. For example, the type of audit to be conducted will determine the selection of audit topics, the identification of audit objectives, the definition of an audit approach, criteria and budgeting and the establishment of the audit team made up of people/staff with the necessary skills and expertise.

An audit plan can now be prepared and the following milestones highlighted to ensure the credibility of the state-level / performance audit process:

- Communication of the audit plan to the relevant stakeholders and approval of the plan;
- Execution of the audit program as agreed among the project team members;
- Reporting of the findings to management;
- Preparation of a public report that includes management responses that outline their plan to address the identified shortcomings;
- Briefing of the executive authority / ministers and tabling of the report;
- Presenting the report to cabinet and the relevant oversight committees;
- Follow-up to ensure that the management commitments are being implemented and the challenges experienced are addressed, giving constructive advice.

3. SURVEY-BASED AUDIT

3.1 Methodology Summary

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.

The questionnaire used in the survey addresses specific information from each of the surveyed organizations, such as governance characteristics, risks involved, controls and results produced in order to build a detailed and broad representation of the organization, which can then be compared to the others. It can be used to assess compliance to multiple legal criteria or to compare business processes to best practices in the field, in the interest of guiding decisions about pursuing further audit enquiries.

3.1.2 What are the Objectives?

Collect information from each organization that is both directly unavailable and relevant to

issue audit recommendations or decide to pursue further enquiries.

3.1.3 When to Use?

Survey based audits are recommended when there is insufficient standardized in-depth information available about a large number of different organizations under the jurisdiction of the SAI. The alternatives to a survey, such as traditional audits on the premises, may not scale well or be too costly in resources. Thus, a survey allows collecting broad information and assessing relevant and associated risks involved in the activities of the target organizations to be able to rank them according to audit priorities and thus allocate scarce audit resources optimally.

3.1.4 Pros / Limitations / Difficulties

Pros: scalability to hundreds of organizations, simultaneously; efficiency in employed resources; can produce large quantities of detailed information; easy replication of standardized questions;

automatic treatment of results; collection of statistics from the population of audited organizations; comparability of results from different organizations; low subjective variability.

Limitations: reliability of collected responses (ambiguity in the interpretation of the questions; noisy data from miscommunication; need to create a strong expectation of control to verify provided information);

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 IT capability); motivate participation in the survey (through command and/or persuasion [free consultancy with ample and specific feedback]); data analysis; specific reporting for every contributor.

3.1.5 Critical Steps / Minimal Requirements

- Require the official assignment of a representative that will be responsible for all communication exchanges between the surveyed organization and the surveying SAI.
- Develop instruments to help participants answer the questionnaire: ample access to the surveying team (email, telephone, meetings); FAQ; references for the survey questions; glossary etc.
- Estimate the burden of answering the questionnaire (also seek comments from the public regarding this estimate). Burden in this context means the time expended by persons to generate, maintain, retain, disclose or provide the information requested.
- Evaluate the use of automated collection techniques or other forms of information technology to minimize the information collection burden.
- Adequate technical solutions to support the survey: web survey (such as Survey Monkey: www.surveymonkey.com, pdf forms or specialized survey software (such as LimeSurvey: www.limesurvey.org).
- Support confidentiality assurances for classified information.
- Provide rich, precise and specific feedback for each organization to keep motivation high

for following surveys. An individual survey report that analyzes organization's responses and compares them to the general population or similar organizations can be of high value and be perceived as a worthy of the effort of responding to the questionnaire.

"A survey will be sent to 1,200 organizations to assess the size, complexity, use of electronic health records, number of locations, how many patient visits and most importantly the fitness of the organization to be audited."

3.1.6 References

GAO – Audit Standards Supplement Series, n° 11, The Audit Survey - A Key Step In Auditing Government Programs (<http://www.gao.gov/assets/180/172676.pdf>).

This standard describes the initial survey of a single activity or program in order to plan and perform a follow-up detailed review. It focuses on identifying problem areas warranting additional review.

Pre-audit survey of the HIPAA program (<https://www.federalregister.gov/articles/2014/02/24/2014-03830/agency-information-collection-activities-proposed-collection-public-comment-request>).

This electronic survey (referred as an Information Collection Request) is considered a pre-audit tool, to determine suitability for a subsequent audit.

It also mentions that some software may need to be installed to collect, validate and verify information.

3.2 Methodology

This section will present the methodology from the concrete experience of Brazil's SAI (TCU) in survey-based audits. Surveys were made in 2007, 2010, 2012 and 2014 to collect information on issues related to the procurement of IT products and services, information security, IT personnel, IT planning and the main governmental systems and databases and general IT governance related information.

3.2.1 Planning

One of the main benefits of periodic surveys is to establish a time line in which the evolution of different metrics can be observed and analyzed. In

this way, results from a given survey are an essential input in the planning of the following survey.

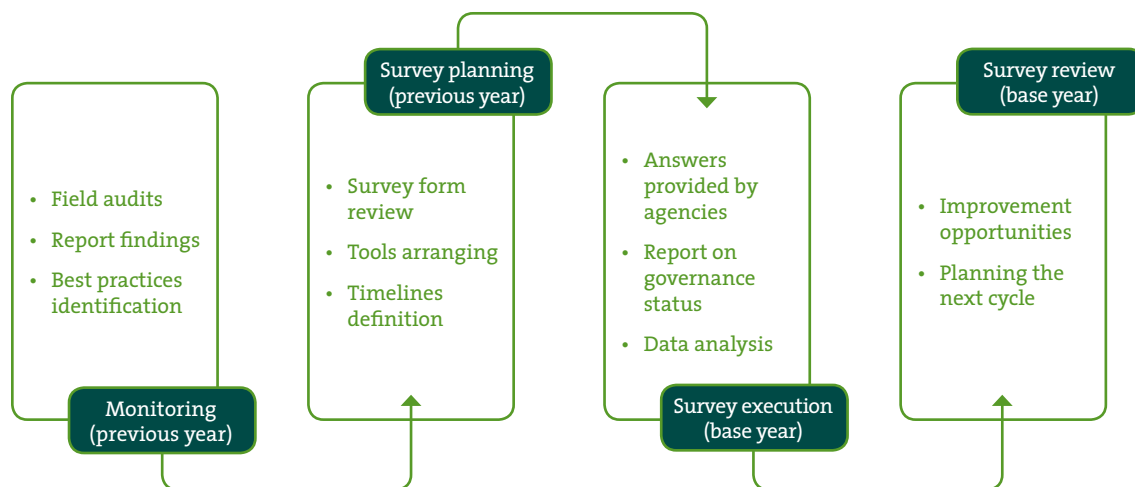
Recognizing this fact, TCU surveys were conducted in even years and their findings are confirmed, in odd years, with audits on a sample of the surveyed agencies that usually find only few inconsistencies in the information provided by the agencies.

The survey process is represented in Figure 4. More details can be found on the SAI-Brazil's case study (Chapter 3, Section 3):

3.2.1.1 Creation / Improvement of the Survey Questionnaire

The creation or improvement of the questionnaire aims to make this assessment tool as didactic and clear in its concepts as possible, considering that one of the main objectives of the survey is to induce in the surveyed organizations a change in behavior, through the emphasis on current legislation and best practices and through signaling the SAIs auditing priorities.

Figure 4: IT governance profile survey



The creation or improvement of the questionnaire must consider:

- criticisms and suggestions made in the previous survey;
- lessons learned from audits that validated the answers to previous survey;
- good practices identified in other organizations or the scientific literature;
- contributions of experts in governance and IT management.

The burden of answering the questionnaire must be estimated and justified in view of the expected benefits resulting from the survey.

There must be planned a phase to submit a draft of the questionnaire to the public, so that anyone can submit comments and suggestions for improving the document and the burden estimate. Then all raised considerations need to be analyzed so that they may be incorporated into the final questionnaire.

There must be an explicit mapping of each question to a reference that supports it: legislation

or other normative instruments, jurisprudence from the SAI or other courts and models of good practice recognized internationally such as COBIT 5 (Control Objectives for Information and related Technology) (ISACA, 2012a), the ISO/IEC 27002 - Information Security (ISO/IEC, 2013) and the ISO/IEC 38500 – IT Corporate Governance (ISO/IEC, 2008).

3.2.1.2 Creation / Selection of the Tools to Help Participants Answer the Questionnaire

In order to assist answering the questionnaire, the following support tools must be developed and published: Glossary, with the definition of key terms; References, with the theoretical background of the questions; and Answers to Frequently Asked Questions.

The use of automated collection techniques or other forms of information technology to minimize the information collection burden has to be evaluated.

3.2.1.3 Selection of Organizations to be Evaluated

Devise the selection criteria to pick the organizations that will be surveyed. These criteria may

relate to budgetary importance, known involved risks, critical functions etc.

Applying these criteria to listing of possible candidate organizations will result in a ranking of priorities and a final selection according to the desired number of survey participants.

The selected organizations may be combined into thematic groups that may facilitate the analysis of their answers and allow the organization to compare its performance to its segment grouping, upon receipt of their individual report. Possible groupings may be state companies; executive, judiciary and legislative branches; third sector.

3.2.2 Execution

The selected organizations must be formally informed of the survey, of its objectives and dates and will be requested to appoint an interlocutor to be responsible of all subsequent communication with the surveying SAI.

It may be desirable to produce an event to present the survey, explain its objectives, clarify the questionnaire, demonstrate possible answers in a case study and gather feedback from the participants.

To implement the survey, seeking to automate procedures for interacting with the participants like a website hosting the questionnaire and related supporting documentation may be necessary. To clarify doubts and allow other direct communications the email address of the survey team may need to be published.

To collect the answers to the questionnaire, taking advantage of survey software (such as the free LimeSurvey, available at <http://www.limesurvey.org>), which allows conducting survey with questionnaires created in the software itself, on a web platform may be an option.

These software offer resources ranging from the request, via email, of the responses to the questionnaire, manage access control by means of cryptographic resources and provide statistical reports of the collected data. These tools also enable controlling deadlines, generate reports on the status of service requests and send messages to warn users about the expired or expiring deadline. The tools can also be used for data validation in the surveyed user's computer through java scripts that may prevent many errors in the answers.

Depending on the length and complexity of the questionnaire, the surveyed must be allowed sufficient time to answer and have means to request a deadline extension.

3.2.3 Reporting Results

Reporting the results of the survey is a key element of the methodology. Effective communication of audit findings allow stakeholders understand the issue without deep or previous knowledge about the subject, as well as allow the auditee capture what is needed to put in place to solve the question.

Every participant in the survey must receive a direct report with a feedback of its participation. In this report, it is desirable positioning the participant within the overall universe of the survey. The communication can be a formal Audit Report, as well as other reporting formats can be used.

Presenting survey results may take several forms, depending on the nature of the data. Usually, surveys lead to qualitative analysis with some sort of categorization. Using bar

charts with categories, frequency distribution histograms or pie charts are common choices. If statistical techniques are used, scattered charts, regression charts and heat maps are also useful tools.

The sections of the questionnaire usually direct analysis and report presentation. Chart dimensions comes from the questionnaire sections, as well as the answer options drive bar charts. If the survey have been repeated from time to time, it is recommended to present the evolution of any topic over time.

It is important to present, from the selected list of participants, who participated and who not participated in the answers. That gives a good idea of the representativeness of the information in the report.

3.2.4 Example of Survey Sections

- Corporate and IT Governance
- Leadership of High Administration

For examples of survey questions, see Tables 1, 2 and 3.

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.					

Table 2: IT Risks Survey

Concerning IT risks:	Adoption level of the practice				
	Doesn't apply	Not adopted	Initiated a plan to adopt	Partially adopted	Entirely adopted
The organization formally defines directives to manage IT risks to which the business is exposed.					
The organization formally defines and communicates roles and responsibilities for managing IT risks.					
The organization formally defines levels of acceptable IT risks on the attainment of its goals (appetite for risk).					
The organization makes strategic decisions considering defined IT risk's levels.					

Table 3: Information Security Survey

Concerning the corporate information security management:	Adoption level of the practice				
	Doesn't apply	Not adopted	Initiated a plan to adopt	Adopts partially	Adopts fully
Policies and Responsibilities					
The organization has an information security policy formally instituted, such as a mandatory compliance standard.					
The organization has an information security committee formally instituted, responsible for formulating and conducting guidelines for the corporate information security, composed of representatives from relevant areas of the organization.					
The organization has an information security manager formally designated, responsible for the information security corporate's actions.					
The organization has an access control policy, for access to information, resources and IT services, that is formally instituted as a mandatory compliance standard.					
The organization has a backup policy formally established as a mandatory compliance standard.					
Controls and Activities					
The organization performs an Asset Management process, ensuring the definition of responsibilities and the maintaining of assets' inventory.					
The organization performs an information classification process.					
The organization implements controls to ensure adequate protection for the confidentiality degree of each class of information.					
The organization performs an Information Security Management process.					

Concerning the corporate information security management:	Adoption level of the practice				
	Doesn't apply	Not adopted	Initiated a plan to adopt	Adopts partially	Adopts fully
Controls and Activities					
The organization performs a technical vulnerability management process, aiming to reduce the risk of exploitation of known vulnerabilities.					
The organization performs a process of monitoring the use of IT resources, aiming to detect unauthorized activities.					
The organization performs an information security incident management process.					
The organization holds, periodically, actions for raising awareness, education and training in information security for its collaborators.					
The organization uses a cryptographic system of digital certification (PKI), to ensure authenticity (authorship and integrity) of information.					

4. IT SELF-ASSESSMENT

4.1 Methodology Summary

4.1.1 What is the Method?

Self-assessment is a powerful way to understand and improve organizational performance, and covers any area of organization's activity, which is evaluated by an organization's personnel with the help of a facilitator or moderator.

The goal of self-assessment is to help the organizations assess the likelihood of achieving their objectives by using the knowledge of the people responsible for meeting them.

This makes self-assessment different from formal and rigid assessment or audit performed by certified assessor or auditor. Having greater risk due to inexperience of self-assessment team and their personal involvement in activities which they evaluate, the positive element is greater knowledge and practical experience about the area they evaluate which helps to identify critical issues and to find proper solutions.

Therefore, it depends a lot on the self-assessment team, on their rigidity and objectivity, criticism towards functions they do perform, commitment to recognize problems and implement improvements.

The first methodological cornerstone is process assessment model, which allows to evaluate present process maturity/capability levels and establish maturity/capability "gaps" needed to cover by improvement activities aimed to achieve established desirable maturity/capability.

Before 2011, for IT-related assessments, CMM-based maturity model was mainly used, developed and published in 2000 in **COBIT® 3rd Edition Management Guidelines** (ISACF, 2000) and used later in COBIT 4 (ITGI, 2005) and COBIT 4.1 (ITGI, 2007) with rich practical examples provided in ITGI publication IT Governance and Process Maturity (ITGI, 2008b).

ISO 15504-based Process assessment model was introduced in ISACA publications initially for COBIT 4.1 processes in 2011 (ISACA, 2011a)

(ISACA, 2011b), and later, in 2013 for COBIT 5 processes (ISACA, 2013a) (ISACA, 2013b).

Both models have their advantages and disadvantages, but they can be used to measure present process maturity/capability levels and set requirements for future process maturity/capability levels.

The second methodological cornerstone is the Goals cascade, which allows linking business goals with IT-related goals and with COBIT processes. This works well as illustrative principle, but in practice, due to specific organizations and their business goals, complex relations with specific IT-related goals and with COBIT processes (having different strength between different bindings, for example) does not allow applying the goals cascade in mechanical way:

“the first step an enterprise should always apply when using the goals cascade is to customise the mapping, taking into account its specific situation. In other words, each enterprise should build its own goals cascade, compare it with COBIT and then refine it” (ISACA, 2012a, p. 20).

Before the Goals cascade appeared in its final form in COBIT 5, business goals, IT goals and their

relations was a subject of research to find their importance and interrelations across different sectors. For example, the publication “Understanding How Business Goals Drive IT Goals”, (ITGI, 2008a) examined business and IT goals over five different sectors, including Government, Utilities and Healthcare Sector and provided prioritized the lists, however strength of linking business goals with IT goals was measured using discrete: “Primary” or “Secondary” relations.

Developed by EUROSAT ITWG, **Methodology for IT self-assessment for SAIs** (EUROSAT 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.

This allows obtaining more precise links between business goals and related COBIT processes, to identify the most important COBIT processes in order to address their maturity issues firstly.

4.1.2 What are the Objectives?

The Self-assessment method for IT function (or ITSA: IT self-assessment) was developed by EUROSAI Information Technology Working Group (EUROSAI ITWG, www.eurosai-it.org) as a tool to assess maturity of IT function at Supreme Audit Institutions of EUROSAI Regional Working Group. The goal of the project was to provide management with some specific insight about the current state of the IT support to their business processes, and how to position future IT for the challenges lying ahead.

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

organization, following methodology, performed required tasks.

Both – methodology and practical workshops – were used to methodologically validate and practically achieve results in the following areas:

- select and prioritize business goals according to their importance to the organization;
- select COBIT processes, which have major influence to selected business goals, and prioritize them according their influence to organization's business goals;
- assess selected COBIT processes using CMM-maturity model;
- find gaps between the future (desired) maturity and the present maturity levels;
- decide on the projects to cover gaps between the present and the future maturity.

4.1.3 When to Use?

Facts and tendencies of the most important business processes and their relations with COBIT processes at the European Supreme

Audit Institutions, validated through practical assessment events, indicates the main strengths and weaknesses of business and COBIT processes, advises how to feel and apply their dependencies.

Method, which is used repeatedly since 2003 in practical IT self-assessment workshops at EUROSAI Supreme Audit Institutions with several events which took place in SAIs of ARABOSAI, AFROSAL-E and AFROSAL-F, may be used at any time at any SAI of the INTOSAI.

Minimum requirement is some knowledge of COBIT, distribution of IT-related activities over COBIT processes and generic and specific criteria for process maturity to achieve certain maturity level.

Application of the self-assessment method in practice allows increasing awareness and competence in IT governance issues, to learn how to apply COBIT for CMM-based assessments, to get feeling how business is related with IT and to strengthen it as long as it is applied in practice.

Even if self-assessment method for IT function was developed for and targeted to Supreme

Audit Institutions and their internal IT function, the main instruments – linking business processes with COBIT processes and COBIT CMM maturity model – are not specific to Supreme Audit Institutions only, and can be extended to any organization and used not only for self-assessment, but for formal assessment activities, including IT audit.

At the National Audit Office of Lithuania IT self-assessment practices, especially increasingly used method of linking business processes with IT processes was one of successfully applied instruments which was used in formal IT audit function, performed at institutions of public sector.

Therefore, not limiting itself to its initial purpose – self-assessment of internal IT function, the method can be used for building external IT audit competence.

4.1.4 Pros / Limitations / Difficulties

4.1.4.1 Pros

- The self-assessment method is universal – it can be applied for any type and size of organization;

- Techniques used by the method – focus on business processes and their links with COBIT processes, selection of most critical COBIT processes – can be adapted and used for formal IT audits;
- Focus on knowledge and expertise of representatives from business and IT to choose and rank the most critical organization's business processes;
- Focus on knowledge and expertise of representatives from business and IT to analyze business processes and on their influence to business processes – this allows to get more precise relations with COBIT processes than “Primary” or “Secondary” estimates, suggested in COBIT;
- The method – if used repeatedly – provides common tendencies and data for analysis – the most critical business processes across different sectors, most typical links with COBIT processes, most significant maturity issues in COBIT processes, best practical solutions to solve maturity issues;
- Self-assessment workshops, attended by business and IT people allows to get

commonly agreed solutions, making IT people better understand business needs, business people – IT strong sides and limitations.

4.1.4.2 Limitations

- The method has no major limitations – the main techniques of selecting and ranking business processes, relating them to COBIT processes, selecting most important COBIT processes – may be used for any organization, and integrated in any type of assessment – from informal self-assessment to formal IT audit.

4.1.4.3 Difficulties

- Requires knowledge of COBIT processes and control objectives, sometimes it is a problem for key business people;
- Requires to know CMM assessment techniques, aligning process-specific maturity criteria to profile of organization (small or big, public or private) and using generic maturity criteria to get more reliable results;
- Missing middle link (IT-related goals) of the business – COBIT processes cascade makes it difficult to link business processes with

COBIT processes directly, especially to assess their level of importance to any selected business process;

- Requires external experienced moderator in cases when self-assessment is performed initially to keep self-assessment process in line with requirements and to assure quality of results.

4.1.5 Critical Steps / Minimal Requirements

Normally, IT self-assessment workshop is executed over the following five agreed stages:

- Organization of the IT Self-assessment;
- Preparation for the pre-workshop meeting;
- The pre-workshop meeting;
- Preparation for the workshop;
- The workshop.

Composition of self-assessment team:

Self-assessment group should be around 12 people (2/3 from business units, 1/3 from IT),

maximum 16 persons. Self-assessment workshop shall be facilitated by 1 or 2 moderators (experts), which could be external or internal, but having sufficient experience and independence.

An important characteristic of IT self-assessment supported by this methodology is the **crucial role of the discussion** during almost every stage **between representatives from the business processes (demand side) and IT-function representatives (supply side)**.

4.2 Methodology

4.2.1 Planning

The planning covers first two (of seven) stages of the IT self-assessment:

- Organization of the IT self-assessment;
- Preparation for the pre-workshop meeting.

4.2.1.1 Stage 1: Organization of the IT self-assessment

Purpose of the **Organization** stage is to ensure that everything is organized for the IT

self-assessment to take place. During this stage, all seven steps (a-g) are executed by the organization performing IT self-assessment. The to-do-list below will help IT self-assessment team to include all the necessary arrangements.

a. Decide to perform IT self-assessment:

- Top-management has to understand importance of IT self-assessment and benefits of it gives to organization; this helps integrate findings of IT self-assessment into regular strategies for IT development of organization;
- Decision to perform IT self-assessment has to be taken by the top-management, planning preliminary dates.

b. Appoint IT self-assessment workshop owner:

- IT self-assessment workshop owner (“Owner”) should be appointed by the top-management, having responsibility for the tasks which are assigned by the top-management activity;
- The Owner can act as IT self-assessment workshop leader on behalf of organization

having responsibility for forming IT self-assessment group, and – in case of external moderators – assures link with them and provides necessary information related to organization and its IT;

- In case the Owner acts as IT self-assessment moderator, he should have sufficient independence from IT function;
- The owner has responsibility to elaborate agenda of the IT self-assessment workshop.

c. Appoint or invite moderators (1 or 2 – to be decided, one moderator can be IT self-assessment workshop owner):

- Moderators shall assure quality and objectivity of IT self-assessment results;
- Moderators may be external or internal;
- Moderators should have good knowledge of IT self-assessment approach and methodology;
- Moderators should be independent, in case of internal moderator, sufficient

independence from IT function should be assured;

- Moderators should speak local language; if not – an international language should be agreed spoken by moderator and participants; in case it is not possible – interpretation should be assured;
- In case there are two moderators, tasks of facilitating the IT self-assessment workshop and documenting should be split.

d. Fix the dates of the IT self-assessment workshop and approving agenda:

- Time should be fixed both for the pre-workshop meeting (0.5 day) and for the main workshop (1-1.5 days); time for meeting with the top management (0.5-1 hour) to report findings of the workshop has to be agreed;
- Pre-workshop meeting may take immediate before the main meeting or some time (2 weeks, for example) before; in that case there will be time for efficient preparation;

- Time needed for preparation by IT self-assessment owner, moderators and participants has to be allocated.

e. Form IT self-assessment workshop group:

- IT self-assessment group should be around 12 people (good proportion is 2/3 from business units, 1/3 from IT), maximum 16 persons;
- IT self-assessment group should know business processes of their own organization;
- Participants from business units should know their business processes well; this is important because they will be the main source of information related of business process needs which are expected to be delivered IT;
- Participants IT should understand business processes and to know how IT can support business goals;
- IT self-assessment group should be familiar with COBIT structure and assessment models, and about business goals

– IT goals and IT processes relations (goals cascade in COBIT 5).

f. Invite IT self-assessment workshop participants:

- Sending IT self-assessment workshop agenda;
- Sending IT self-assessment methodology;
- Sending COBIT and other relevant information to IT self-assessment workshop participants, indicating what are important points to read to prepare for the workshop; at this stage its worth to mention business processes and how IT can support them.

g. Prepare the meeting room and logistics:

- Meeting room;
- 2 computers (1 connected to video projector for demonstration; 1 connected to printer for documentation of results);
- Flipchart and pens;
- Handouts of presentations;

- Copies of empty forms to be filled in by the participants;

- Copies of evaluation forms;

- Lunch, coffee, tea etc.

4.2.1.2 **Stage 2: Preparation for the pre-workshop meeting**

Purpose of the **Preparation stage** is to assure that participants and moderators are well prepared and have a common frame of reference when the pre-workshop meeting starts.

a. Preparation by moderators:

- Get familiarized with the self-assessment methodology;
- To know COBIT framework, processes and control objectives, assessment models; generic and specific metrics to measure process maturity or capability;
- Study documents provided by the organization to understand the main business processes and IT processes supporting them, activities, risks and controls;

- Any other information related to policies, plans, laws, regulations and contracts, results of previous audits, problems and challenges expected to arise in the future;
- Prepare or adapt PowerPoint presentation to be used during the self-assessment workshop to introduce method to the participants.

b. Preparation by participants:

- To understand the main business processes;
- To understand COBIT framework and assessment models;
- To understand how IT processes support business goals, understanding COBIT goals cascade would be an advantage.

c. Preparation by IT self-assessment workshop owner:

- If the Owner is moderator at the same time, he has to be prepared as workshop moderator;

- To know well the main information about organization, its policies, plans, laws, regulations and contracts;
- Any other information related to policies, plans, laws, regulations and contracts, results of previous audits, problems and challenges expected to arise in the future;
- To understand well the main business processes, both primary and secondary;
- To know COBIT framework and assessment models;
- To understand how IT processes support business goals, understanding COBIT goals cascade would be an advantage.

4.2.2 Execution

The execution part covers the following 3rd -5th stages:

3. The pre-workshop meeting;
4. Preparation for the workshop;
5. The workshop.

4.2.2.1 Stage 3: Pre-workshop meeting (4h)

Purpose of this stage is to ensure that the participants become well informed about what the IT self-assessment is about, that they have the right expectations of its outcome and that they are well prepared when the workshop starts.

One of the main objectives is to stimulate the participants to prepare themselves for the workshop, outcome of this stage – an understanding by the participants of the background of the IT self-assessment, its objectives and the value of its results for their SAI.

Participants are aware of their role in a self-assessment and of the role of the moderators.

During this stage, the following six steps (a-f) are executed:

- a. Introduction of moderator and participants (30 min): participants and moderator are expected to introduce themselves, mentioning their name, their position within the SAI and their experience in areas like auditing, IT and the use of COBIT;
- b. Introduction of expectations and purpose of the IT self-assessment workshop owner (45 min): some participants are invited to present their ideas about the importance of IT governance for their SAI and about the consequences of this importance. This step includes a discussion between participants;
- c. Presentation of the various steps (45 min):
 - Role and contribution of IT self-assessment to institutional capacity building;
 - Explanation about COBIT-based self-assessment, how evaluating process present and future maturity can facilitate IT actions, supporting the main business of the organization;
 - IT self-assessment: short presentation of the various activities and the way in which they are mapped into stages;
 - Conclusions and questions.
- d. Introduction of the Business Value Chain (BVC) form and business processes (30 min): the various columns of the BVC form

(Figure 5) are introduced so that the participants will understand their meaning and will be able to work on the assignments after the pre-workshop meeting:

- Business processes and related information systems or development projects;
- Actual importance of IT for this process (score 0 – 5): how strong business process depends on IT at present; for example: 0- IT is not important; 1- IT used on Word/Excel level; 2- simple applications; 3- complex applications; 4- IT systems; 5- complex IT systems;
- Future importance of IT for this process (score 0 – 5): what is expected dependence of business process on IT in the future;
- Actual quality of IT for this process (score 0 – 5): low quality should indicate low maturity grades of related COBIT processes;
- Kinds of experienced problems (score 0 – 5): problems may be caused by poor functioning of IT, also may be other causes.

- e. Introduction of COBIT framework with focus on IT-processes (45 min): this step is extremely important, because after the pre-workshop meeting the participants are expected to be able to determine relevance of the various IT-processes to business goals of organization. Participants should have read at least introduction to the framework to understand the main concepts. However, it is desirable to explain structure of process domains and IT processes, indicating for what specific process is responsible and how to assess its maturity.

After this short introduction of COBIT, the various columns of the COBIT form (Figure 6) will be explained:

- Importance of the process (score “not known”, 1 – 5): how strong IT process is linked to one or some business processes, idea is like “primary” or “secondary” relations in COBIT 5 goals cascade, but more accurate measure of dependence (from 1 to 5);
- Actual maturity level of this process (score 0 – 5): maturity is measured using process specific CMM models using 0.5 maturity scale;

- Desired (or future) maturity level of this process (score 0 – 5): desired maturity level will be set by the self-assessment group, maturity is measured using process specific CMM models using 0.5 maturity scale;
 - Business processes that may be influenced by a low actual maturity of IT processes: links to identified business processes which are already indicated in the BVC-form.
- f.** Assignments to participants and closing (15 min): Explaining how workshop participants should fill the BVC form (Figure 5) and how to determine importance of COBIT processes, filling the first column of COBIT form (Figure 6).
- actions to be taken to cover maturity gaps). The following two steps are executed:
- a.** Preparation by workshop participants: Filling in the BVC form (Figure 5), determining importance of COBIT processes and filling the first column of COBIT form (Figure 6);
 - b.** Preparation by moderators:
 - importing individual BVC form scores into the BVC consolidation spreadsheet (Figure 8);
 - few statistics are calculated to provide business process overview;
 - importing individual scores related to COBIT process importance to COBIT consolidation sheet (Figure 9);
 - sorting Excel sheet based on the (decreasing) importance of the IT-processes.

4.2.2.2 Stage 4: Preparation for the Workshop

Purpose of this stage is to ensure that the participants fill in their scores in BVC and COBIT forms and pass the results to moderators, which input them into consolidating spreadsheets. Moderators will use those results during the main part of workshop – discussions, maturity assessment and gap analysis (discussion on

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

Purpose of this stage is to measure process maturity, find out maturity gaps and design

an action plan that covers the most important gaps in the IT function so that business processes in the future will be better supported by IT.

During this stage, the following seven steps (a-g) are executed:

- a. Introduction (15 min): a short recapitulation of what has been done so far and a presentation of the workshop agenda;
- b. Presentation of the BVC-analysis and discussion (60 min):
 - Moderators analyze individual scores of the BVC form and present some statistics (arithmetical average is calculated) (Figure 8);
 - Group discussion related to the results: a group consensus has to take place during the workshop, in order to come to an agreement about the scores. Participants should express their opinion and arguments in case their scores are marginal;
 - Documenting evidence related to the agreed scores.
- c. Presentation of COBIT processes analysis and discussion (45 min):
 - Moderators analyze individual scores (Figure 6) regarding importance of COBIT processes and present some statistics (arithmetical average is calculated) (Figure 9);
 - Group discussion related to the results: a group consensus has to take place during the workshop, in order to come to an agreement about the scores. Participants should express their opinion and arguments in case their scores are marginal;
 - Documenting evidence related to the agreed scores.

The outcome of this phase is participants reaching an agreement about the level of present and future IT-support and about the quality of the present IT support of the business processes. Moreover, they become aware of which IT-processes directly or indirectly support business processes.

The outcome of this phase is participants reaching an agreement about the level of importance of COBIT processes. A limited number of the

most important COBIT processes (maximum of 15) is selected for future maturity analysis.

d. Determining maturity levels of selected COBIT processes (90 min):

- Each participant assesses all selected COBIT processes to determine their maturity using process-specific assessment criteria (Figure 6);
- Group discussion related to the results: a group consensus on the identified maturity levels (Figure 9). For each COBIT process, the following information is recorded;
- Actual maturity level;
- Shortcomings: what is not fulfilled to achieve higher maturity level;
- Risks associated with shortcomings;
- Business processes affected by COBIT process investigated (“goals cascade”);
- Future maturity levels shall be discussed (Figure 9), taking into consideration that

significant maturity gaps (difference between future and present maturity) are more expensive to cover (improvement initiatives are longer and more difficult);

- After future maturity level is agreed, maturity gaps are identified.

NOTE:

- Maturity score may be either the arithmetical average of all participants’ scores or commonly agreed during discussion;
- Metrics for maturity level may be different and moderator should know different options of maturity measuring (level x means that all criteria set for level x are fulfilled; or level may be calculated as a (weighted) arithmetical average of all fulfilled criteria calculated in all levels from 1 to 5). CMM maturity metrics are described in (ISACA, 2003), also in Maturity Toolkit attached to publication (ISACA, 2009);
- Workshop owner or moderator should consider using tools to assess maturity. Some maturity assessment excel sheets attached to that publication may be used or adapted.

- e. Design of the action plan (120 minutes): the purpose is to produce a list of actions (projects) for promoting improvements, including documented evidence related to priority-setting, based on benefits/advantages and costs/drawbacks analyzes:
 - Introducing the Findings and action form (Figure 7) and what has to be filled in;
 - All maturity gaps are recorded using the Findings and action form;
 - Actions to cover maturity gaps are discussed and priorities (scale 0..10) are assigned considering two components:
 - » 1) expected benefits (more important for business: higher priority); and
 - » 2) implementation costs (lower cost: higher priority); priority is given to actions with higher sum of the two components;
 - Owners of actions are identified, risks to implement those actions are discussed and deadlines for implementation of those actions are established;
 - The action plan is made ready to be presented to top management of the organization.
 - f. Evaluation (30 min): the purpose is to get an overview of the participants' opinions related to the various aspects of the workshop (experience, benefits, composition of groups, difficulties etc.). A Feedback form is distributed and filled in by the participants.
 - g. Communication of results (30 min): the purpose is that top management be informed about what has been done during the workshop and what it delivered for their organization. It is a presentation describing the process of the IT self-assessment and its findings.
- The formal report has to be issued after the IT self-assessment is done, documenting the process and its outcomes, including relevant background, context and performance.
- IT self-assessment should be considered as a normal institutional activity and repeated as a tool for continuous improvement of the IT governance.

4.2.3 Main Documents / Forms Required for Self-assessment

Figure 5: BVC form

Questionnaire 1: Does the IT help to achieve the SAI's strategic goals?					ACTUAL quality of the computerization of this process?				
version 4.0					What kind of IT-problems are existing within this range (especially if the range of the quality level is 0 or 1)?				
ACTUAL importance of the IT for this process?					FUTURE importance of the IT for this process?				
no application software (0)					no application software (0)				
low (1)					low (1)				
importance level (2)					importance level (2)				
importance level (3)					importance level (3)				
importance level (4)					importance level (4)				
high (5)					high (5)				
☐	B1	Business process 1	related application software or project						
	B2	Business process 2	related application software or project						
	B3	Business process 3	related application software or project						
	B4	Business process 4	related application software or project						
	B5	Business process 5	related application software or project						
	B6	Business process 6	related application software or project						
	B7	Business process 7	related application software or project						
	B8	Business process 8	related application software or project						
	B9	Business process 9	related application software or project						
	B10	Business process 10	related application software or project						
	B11	Business process 11	related application software or project						
	B12	Business process 12	related application software or project						
	B13	Business process 13	related application software or project						
	B14	Business process 14	related application software or project						

Figure 6: COBIT form

IMPORTANCE of this process?					Questionnaire 2: IT-Processes. How mature are the IT-Processes?		ACTUAL maturity level of this process?					DESIRED maturity level of this process?					Which business processes (Questionnaire 1) might be influenced because of this condition (in particular if the maturity level is deep, i.e. 0 or 1)?	
					version 4.0													
not known	not important (1)	importance level (2)	importance level (3)	importance level (4)	importance level (5)		non-existent (0)	initial / ad hoc (1)	repeatable but intuitive (2)	defined process (3)	managed and measurable (4)	optimised (5)	non-existent (0)	initial / ad hoc (1)	repeatable but intuitive (2)	defined process (3)		managed and measurable (4)
Domains and IT-Processes following Cobit 4.0																		
Plan and Organise																		
						P01	Define a Strategic IT plan											
						P02	Define the Information Architecture											
						P03	Determine Technological Direction											
						P04	Define the IT Processes, Organisation and Relationships											
						P05	Manage the IT Investment											
						P06	Communicate Management Aims and Direction											
						P07	Manage IT Human Resources											
						P08	Manage Quality											
						P09	Assess and Manage IT Risks											
						P010	Manage Projects											
Acquire and Implement																		
						A01	Identify automated solutions											
						A02	Acquire and maintain application software											
						A03	Acquire and maintain technology infrastructure											
						A04	Enable operation and use											
						A05	Procure IT resources											
						A06	Manage changes											
						A07	Install and accredit solutions and changes											
Deliver and Support																		
						DS1	Define and manage service levels											
						DS2	Manage third-party services											
						DS3	Manage performance and capacity											
						DS4	Enable continuous service											
						DS5	Ensure systems security											
						DS6	Identify and allocate costs											
						DS7	Educate and train users											
						DS8	Manage service desk and incidents											
						DS9	Manage the configuration											

Figure 9: Sample COBIT consolidation form

COBIT Form 2 - Consolidation																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																							
Process	Importance of the process ?													Current maturity level of the process ?													Desired maturity level of the process ?																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																												
	participant 1	participant 2	participant 3	participant 4	participant 5	participant 6	participant 7	participant 8	participant 9	participant 10	participant 11	participant 12	participant 13	total	average	average (d2)	participant 1	participant 2	participant 3	participant 4	participant 5	participant 6	participant 7	participant 8	participant 9	participant 10	participant 11	participant 12	participant 13	total	average	average (d2)	participant 1	participant 2	participant 3	participant 4	participant 5	participant 6	participant 7	participant 8	participant 9	participant 10	participant 11	participant 12	participant 13	total	average																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																								



CASE STUDIES

Chapter

03

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.

1. STATE AUDIT BUREAU OF KUWAIT

“INDIVIDUAL ORGANIZATION” METHOD

1.1 Summary

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. The IT Governance audit was performed in the form of IT Performance Audit on the management of information systems and with more focus on (HIS) and the real reasons behind the decision to replace it. The State Audit Bureau work resulted in producing twelve major recommendations that are aimed at assisting the new (HIS) procurement process and improving the efficiency and effectiveness of the future (HIS) by avoiding past pitfalls.

After 1 year, the State Audit Bureau conducted a follow-up study in order to investigate the response that resulted from the initial recommendations.

1.2 The SAI

The Constitution of the State of Kuwait, which was issued on November 11, 1962, clearly provided for the establishment of a commission for financial control in which its independence shall be safeguarded by the law. Believing that public funds, that form the State's nerve and its cornerstone for prosperity, should be safeguarded to insure full collection of revenues, avoid any loss or negligence and expend these revenues for the welfare of the society without extravagance or unreasonable economizing. The main objective of SAB is to maintain an effective control over the public funds to safeguard them, prevent any misuse, and verify their proper utilization for the purposes they have been allocated.

Through performance of its control activity, SAB has concentrated on the creation of a full conviction over the audited bodies. That is, SAB is not looking for errors or deviations; instead, it aims primarily at the maintenance of public interests by safeguarding public funds and

efficiently utilizing them for the aspects they have been allocated.

In order for SAB to actualize its objectives, two different Audit procedures were developed to serve as safeguard mechanisms, which are practically deployed around two phases of a commitment. One is practiced before a commitment (Pre-Audit) and another after a commitment (Post-Audit). A third type has also been developed in order to serve as an empowerment and a support tool (Performance Audit) and, in this type, the concept of Governance is implemented.

Performance Audit for IT is oriented towards studying areas of the IT universe, management, control and governance. It may be described as an independent auditing process aimed at evaluating the measures instituted by management, or the lack of these measures; ensuring that resources have been acquired economically and are utilized efficiently and effectively.

Such audits are specialized in the benchmarking against international IT standards and guidelines. Thus, performance audits reports are fashioned in a way to provide guidance to the auditee on how to improve on the area under review.

1.3 The Challenge

Through the initial audit, it was found that the IT department in charge of (HIS) had no clear work programs to measure its performance or efficiency. This made it difficult to effectively pursue improving the system's performance by making the correct decisions in the right time. Additionally, the department did not employ a mechanism to execute plans related to performance measurements for the system or any other project. Nor was there a method to manage projects or evaluate their progress. All of this evidently, was found to be the result of the lack of policies surrounding the procurement and management of IT systems. The current (HIS) is now lacking desired functionalities, inefficient, hard to manage and costly to improve on.

Looking at the effort of the department for the process of decision-making to replace the (HIS), there was not even ad hoc procedures for risk management or feasibility studies let alone any officially adopted frameworks. In addition, the future (HIS) RFP currently in the works lacks the standard work of proper requirements study that reflects communication with the users here being the different medical departments

while considering all their needed applications and operational differences.

There was also an inherent problem to the establishment itself because it does not abide to many of the public health rules, regulations and standards. The hospital was built to serve the employees and their families of the company and its 11 subsidiaries; thus, it is under a total independent management from the Ministry of Health that supervises the public hospitals. This makes the hospital and its management isolated and does not participate in any exchange of experiences that naturally happen between other public hospitals. In addition, it is a non-profit hospital so it has no experience gained through a commercial practice. This unique situation made the hospital lag behind other hospitals in managerial experience and problem solving skills. Naturally, this is reflected on (HIS) and results in its current state.

1.4 What Was Done

The State Audit Bureau conducted an IT Governance audit based on the General Guideline of Performance Audit developed and adopted internally. Much of the performance

audit on IT in the guideline is derived from the COBIT framework and adapted to governmental use. The audit was carried out through a series of reviews of the available documentations, interviews with concerned parties, site visits, inspections and questionnaire evaluations.

The audit at first, focused on areas that can provide relevant results in understanding the situation around the current (HIS). Areas like, work programs, project management and risk management were investigated. This resulted in the following recommendations:

- It is necessary to implement clear work programs in the IT department to measure the performance and investigate the efficiency that should assist in achieving an effective follow-up, appropriate corrective actions and improvement of performance in a non-reactive way;
- The importance to adapt a mechanism/standard to manage IT projects that should make it more efficient to monitor and measure the performance of executing projects, evaluate milestones, correct progress paths and issue periodical reports on performance and commitment to delivery;

- To prepare IT policies regarding the development/procurement and monitoring of systems in order to insure positive outcomes;
- To adapt a risk management program to discover and analyze risks resulting from the use of developed/procured systems and assist in implementing suitable controls.

Then the audit focus was further narrowed in order to assist the process of procuring the replacement (HIS). Fortunately, the department was in the stage of putting down the RFP for a tender. The following recommendations were given:

- Prepare a ROI (return on investment) study for the hospital in light of the projected costs due to the use of the new advanced technologies;
- Prepare a feasibility study on the (HIS) replacement project for the hospital while keeping in mind the execution capabilities in light of the desired objectives;
- Specify and document the requirements of the different organizational units. Covering systems, applications and electronic medical equipment necessary for operation while considering the different applications and duties of medical units. Additionally, the department needs to generate dataflow diagrams in order to better meet the user requirements and assure proper data integration and effective operational controls;
- To make use of the accumulated experience from working with the current (HIS) and analyze the current situation in order to pinpoint current major issues that necessitated the replacement decision;
- To coordinate with the Ministry of Health and initiate an experience exchange program to learn more about the use of information technology in the public hospitals;
- To coordinate with all concerned parties in order to realize the desired benefits from the new (HIS) while adhering to the assigned budget and target deadline as much as possible;
- To employ an up-to-date operational method, data integration and exchange in a unified method across all medical units within the hospital and to prepare appropriate planning for the following:

- a. Data migration from the retired (HIS) to the new one;
 - b. Integration of the planned (HIS) with other systems, if needed;
 - c. Proper user acceptance testing process with sufficient scenarios in coordination with the user.
- To adapt and adhere to a periodical audit/monitoring processes to ensure the maximum utilization of the new (HIS) and come up with new recommendations.

1.5 Evolution

One year after providing the IT department with the recommendations, a follow-up audit was performed to evaluate the situation and see how much of them were actually beneficial. This time the audit was carried out again through reviews of the available documentation, interviews with concerned parties, site visits, inspections and questionnaire evaluations.

It seems that the previous recommendation have put the department on the right track as it has went as far as establishing a quality control unit under the information technology

planning team. The department has also developed a work plan for the quality control unit and currently going through the process of acquiring the ISO 9001:2008 qualification. In addition, the department has developed and demonstrated strategic, operational and work plans that were found to be sufficient and reflect a decent maturation of the department.

As for project management, the department supported many of its senior staff to become PMP certified and in addition to that, it has deployed and trained its staff on the use of Microsoft Project Server. The department was also keen enough to point out that this initiative must only be considered as a starting point, as it realizes that project management must and will also be adapted to fit the special needs of the organization.

The department has made a strategic decision regarding acquiring software after it had realized through an in-house initiated study that it would be less costly, easier to support and more efficient to procure over the shelf applications and customize them rather than to develop its own. This came by recognizing that the field of information technology is an already mature field and offers even more than what the

department needs and allows it to focus on its medical field. Therefore, the department proceeded to develop procurement standards that are in parallel with its new project management process.

Regarding risk management, it turned out that the department has not addressed this area yet. Nonetheless, it initiated a preliminary risk analysis study on delaying work programs. Even though this is considered a critical issue delay but nonetheless, the department's initiative should lead to something better in the future. Another area that the department have not worked with yet is ROI studies as it has clearly stated that such analysis are not a major concern because the hospital is non-profit and fully funded by the government. The state Audit Bureau sees this as a no excuse and ROI studies are still highly recommended.

The department demonstrated that feasibility studies have become a standard practice; again stemming from the new project management process. The State Audit Bureau have received and reviewed the feasibility study that was carried out for the replacement (HIS), which is believed to have helped in a successful new environment.

The results of the State Audit Bureau recommendations have proved to have a positive propagating effect. Due to the department's strategic decision to avoid in-house development of software, the recommendation for documentation is now inherently adhered to since ready-made software come with proper full documentation.

During the follow-up audit, the department presented a full report on the situation of the previous (HIS), assessing the major issues and reasons for replacement. At this point, it is necessary to reference that the department also initiated an experience exchange program with the Ministry of Health. Site visits, meetings and workshops were conducted with IT departments of public hospitals. Both the study of the previous (HIS) and the experience exchange were great assets in helping deploying the new (HIS).

The department has also shown how the new project management process is inclusive of the requirement to coordinate with all concerned parties surrounding a project. It had provided the audit team with documents showing that all concerned parties were included and well communicated during the course of new (HIS).

As for the recommendation regarding operational methods, the department has not taken much action nor did it provide any feedback on it. The department sufficed with pointing out that the project management process already covers for that which is not true. The Data migration, integration and acceptance testing are technical subjects and cannot be covered by project management only. It is possible, though, those such technical issues were trusted to the vendor since the new (HIS) is an off-the-shelf product, supported by its supplier.

The department has implemented a periodic process of independent audit and performance monitoring for all the department's systems. Additionally, the department provided us with a review report on the new (HIS) to confirm achieving the desired goals. The review was conducted six months after the deploying the (HIS) and it shows success in both achieving results, relieving staff from unnecessary burden and easing the users experience.

1.6 Key Messages

- In some situations, IT governance can be applied in a selective way with a narrow focus in order to serve a more short-term or immediate need;
- IT governance concepts complement each other and sometimes act as a catalyst of change in many different areas. This was the case when looking at how the project management affected different aspects of governance in the case study. Another example was the strategic decision of acquiring ready-made software and its benefits in providing inherent governance regarding documentation and operations;
- Experience exchange and exposure to relevant industry is a key driver in the maturity of IT in general;
- The public sector has common difficulty with the concept of ROI, especially when it lacks providing services/products or if it is a non-profit organization.

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 to suggest 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 well as practical is their implementation at the NAO LT. Actively using COBIT since 2003, the NAO LT brings the framework to the public sector in its live form, sharing its own practices starting from IT function gaps analysis for IT strategies up to application of COBIT goals

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 becomes a competent adviser to the Government.

2.2 The SAI

The National Audit Office (the State Control) of Lithuania was established in 1919 and appointed the first State Controller Kostas Daugirdas. After the Restoration of the Independent State of Lithuania in March 1990, the National Audit Office of Lithuania (then the State Control Department) was restored in April 1990. In October 1992, the Supreme Control Institution

of the Republic of Lithuania (the State Control Department) was admitted as a member of INTOSAI (www.intosai.org).

Subsequent adoptions of the Law on the State Control of the Republic of Lithuania brought more power and independence. Having adopted the Law on the State Control in 1995 and its amendments in 1998, the organizational structure of the State Control was further developed and new working methods based on the best international practices were introduced. In 2001, The Law on the Amendment of the Law of State Control was adopted, defining the National Audit Office as the supreme government audit institution, accountable to the Seimas (the Parliament). Public Auditing Requirements, based on INTOSAI's and other international auditing standards, were approved, shifting activities' focus from control to audit and introducing value-for-money auditing.

The topic of IT governance appeared at the National Audit Office of Lithuania in 2002, when the EUROSAI IT Working Group was founded and the NAO was among the members of the project "ITSA – Information Technology Self-assessment as a management

support instrument", devised to create a methodology for COBIT-based self-assessments and to conduct moderated self-assessment workshops across the working group members.

The first self-assessment workshop of the ITSA project (and the first one in the EUROSAI region) took place in Lithuania, in October 2003. Based on maturity gaps, improvements to NAO's IT governance were made, such as the establishment of an IT Management Committee, which meant hierarchy of business over IT concerning IT-enabled business solutions. The second self-assessment happened in 2006 and identified maturity gaps – weak points to be considered by the NAO's IT strategy for the period 2007-2011. The third self-assessment occurred in 2015, analyzed maturity of the most important COBIT processes, which appeared in the NAO's IT strategy for 2015-2020, which was worked out using COBIT philosophy and goals cascade while deriving NAO's IT goals from NAO's business goals (The National Audit Office of Lithuania, 2014).

The IT Audit function and corresponding structure were established in 2006, with the proprietary IT Audit Guidelines, where most of the procedures are linked to various

COBIT guides and ISACA publications. Based on practical audit experience, in 2012 the IT Audit Guidelines were reworked, and IT Audit Manual was released.

2.3 The Challenge

In the public sector, IT governance objectives may not be achieved at each institution, even if their own IT governance is efficient and effective. Working at different administrative levels and being dependent on each other, activities of institutions may be a part of a more general IT governance initiative and, if they are not properly positioned (evaluated, directed and monitored) by the higher level, IT governance results at the lower level may be useless due to incorrect direction taking.

Therefore, one should not evaluate a single institution and its local results only, but, instead, go to the highest possible level in order to verify if the necessary legislation is enforced, a proper IT governance framework is set, relevant IT governance initiatives are released at the highest level and results of IT governance programs are adequately monitored to get lessons learned for new directions.

Lithuania's NAO addresses these questions during its IT governance audits, as explained below.

2.4 What Was Done

According to the IT Audit Manual, IT governance audit is performed at the following levels:

- IT governance issues of simple information systems are assigned to financial auditors, who assess them based on questionnaires developed during their financial audits. This contributes a lot to the efficiency of IT auditing: structured information brought by financial auditors from hundreds of auditee institutions gives an exhaustive picture of the basic information systems control environment in the public sector;
- IT auditors use the findings obtained by financial auditors, generalizing and testing them in specialized IT audits of more complex IT systems. In such audits, they try to answer the questions below:
 - a. What are the auditee's IT governance problems/maturity issues?
 - b. Are these problems related to inadequate efficiency of IT governance?

- c. Are there any legal obstacles preventing the auditee from achieving its IT governance objectives?
- Once every 5-6 years, IT auditors perform a supra-ministerial IT governance evaluation, assessing if the state has adequate legal and managerial capacities or mechanisms in place to assure an effective and efficient IT governance framework is implemented at the ministerial level. In this case, audit recommendations go to the Prime Minister's Office and the main issues are related to legislation improvements (imposing of better IT controls and better structures/responsibilities for coordinating IT governance functions, including state-level IT programs defining, financing and prioritization).

In that respect, COBIT philosophy was applied and accordingly adjusted to the public sector's reality. Its main principles (business should get value from IT investments, IT strategy should be aligned to the business strategy etc.) remained valid, while the auditor's perspective needed to shift from auditing an individual organization to auditing the whole government (state-level audit).

That was achieved by looking at the central government as the overall "organization" and at the ministries as different "business units". The central government's existing committees and commissions were treated like "IT Strategy" or "IT Steering" committees within traditional organizations.

Planning and monitoring principles were extended from an institutional to a governmental level. Principles regarding governance improvement were adapted from ISO/IEC 38500:2008 and the COBIT 5 framework. Responsibility to stakeholders was treated as responsibility to citizens. The concept of "governance" was relocated to the governmental (political) level, since the government is equally required to evaluate and monitor when setting direction based on political initiatives.

Similarly to what happens within an individual organization, when we talk about the public sector as a whole, if IT governance is not carried out according to evaluate-direct-monitor principles, management processes may not lead to the desired results, independently of how effective and efficient they are.

Therefore, auditing IT governance at the supra-ministerial level is important to suggest mechanisms for proper IT governance at the highest level.

2.5 Evolution

National Audit Office of Lithuania has started with two IT governance state-level audits, one in 2006 (“General Control of State Information Systems. State and Institutional Levels”) and another one in 2007 (“Management of Information Systems of Public Institutions in the Context of E-Governance”).

The aim of both these audits was to evaluate general controls at the state level, i.e. if the state had adequate legal and managerial capacities or mechanisms in place to assure an effective and efficient IT governance.

Recommendations were issued and aimed at:

- Strengthening legal regulations regarding IT governance (preparing a new law on governance and management of information resources and subsequent regulations stipulated by this law);
- Reviewing, updating and assuring compatibility between long-term IT strategic documents, enforcing an IT strategic planning culture and the necessary instruments (for example, IT Strategy Committees);
- Providing ministries/governmental agencies (those having responsibilities aspects of state regulation) with the necessary powers of administrative control and monitoring (for example, assuring continuous monitoring of IT investment projects, considering their efficiency and effectiveness).

The outcome of these audits was the new Law on Management of State Information Resources (2011), which provided a framework for better IT governance. Nevertheless, subsequent secondary legislation had still to be enforced.

In 2013, another audit (“Governance of State information Resources”) was conducted, aiming to evaluate the IT governance framework enforced by the mentioned law and to suggest improvements on legal and/or financial related instruments.

Recommendations were issued to the Government of Republic of Lithuania, aiming at:

- Improving the IT governance model by applying governance methods suggested by Lithuanian and international best practices standards and recommendations:
 - a. developing a consistent classification scheme regarding state information resources, based on common principles;
 - b. complementing the implementation plan of the Law on Management of State Information Resources, including provisions related to reviewing and conformity-assuring of existing legal acts;
 - c. developing and applying unified goals and performance criteria for IT management and security across all areas of the government.
- Assuring common policies for governance of information resources:
 - a. foreseeing measures for better coordination of the information resources policies' implementation;
 - b. appointing an institution responsible for coordinating classified information and compiling an inventory of such information;
 - c. assuring priorities for IT investments are established at the governmental level;
 - d. compiling and publishing information on state-owned information networks.
- Assuring financial resources are efficiently used and investments are aligned to the main trends of IT development, to elaborate:
 - a. regulatory and control measures for centralized planning of the most important IT projects; these measures should assure cost-effectiveness, technological compatibility, evaluation of impact and monitoring at the state level;
 - b. requirements to evaluate the possibility of adapting IT systems or solutions already existing at the public sector;
 - c. requirements for planning of IT financial resources.

Most of these audit recommendations are already implemented, which created a new improved legal framework for IT governance in Lithuania.

2.6 Key Messages

- Use widely known and open audit methodologies (COBIT, for example), as well as tested parameters and largely accepted governance/management practices (not invented by you) as criteria;
- Recommend good practices tailored to the auditee's specific reality and context in order to facilitate him to improve his IT governance; preferably, try to make recommendations that will effectively bring positive changes rather than merely pointing out compliance/non-compliance situations according to legislation;
- Recommend to the auditee practices, methods and tools you know well and, ideally, have already applied in your own SAI; this way, you demonstrate having practical (not only theoretical) knowledge and expertise;
- Continuously acquire knowledge and get internationally recognized certificates (they prove your competence);
- Conquer the auditee's trust and confidence by demonstrating your competence and proposing tailored good practices and real-life tested recommendations; show him you are a partner, not an enemy, in his IT governance improvement process;
- Always test the highest possible IT governance levels, since the reasons of unsatisfactory IT governance within the organization may be external (for example, caused by the inheritance of an unfavorable IT governance framework or by the inability of higher IT governance instances in evaluating, directing and monitoring IT governance initiatives).

3. FEDERAL COURT OF ACCOUNTS OF BRAZIL

“SURVEY-BASED” METHOD

3.1 Summary

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.

After four editions of the IT Governance Survey conducted by TCU (2007, 2010, 2012 and 2014), data collected shows that all these efforts have effectively improved the results obtained by organizations, while reducing the risks that they are exposed to.

3.2 The SAI

TCU audits the accounts of administrators and other persons responsible for federal public funds, assets and other valuables, as well as the

accounts of any person who may give cause to loss, misapplication or other irregularities that may affect negatively the public treasury.

TCU is a collegiate body made up of nine ministers (six are chosen by the National Congress; three are selected by the President of the Republic, upon the Senate’s approval). The Court has a Secretariat that provides the necessary technical and administrative support in order for it to carry out its constitutionally and legally mandated attributions. This Secretariat is divided into several technical and executive units responsible for auditing the use of federal funds, and these units are located in Brasilia (Brazil’s capital) and in the 26 States of the Federation. One of these units is the Department of External Control - IT (*Secretaria de Fiscalização de TI – Sefti*), created in 2006.

TCU has successfully endeavored to keep up with the evolution of society’s demands and recent changes in the public sector, as well as to stay up-to-date with IT advances, continually improving its systems to position itself as one of the leaders

in the application of modern resources and procedures applied to external control. Its objective is to ensure the ongoing and effective administration of public funds for the benefit of society.

3.3 The Challenge

The purpose of information technology governance is to ensure that IT projects are in line with business objectives and add value to the organization. The performance of IT department should be measured; their resources properly allocated; and their inherent risks mitigated. In this way, IT initiatives can be managed and controlled in organizations to guarantee returns on investment and improvements in organizational processes. Appropriate information technology governance in the federal government allows the protection of critical information and contributes to the attainment of organizations' institutional goals. Nevertheless, most audits showed recurring problems over procurement, high vendor dependency, lack of skilled personnel, lack of planning and failure of IT projects due to deficiencies in IT governance. Thus, in 2007, TCU needed to know how was the maturity level in each IT governance aspect to focus its audit efforts in most relevant issues.

3.4 What Was Done

TCU's goal is to audit the use and management of IT resources in the federal government and to promote improvements in IT governance. To this end, it needs to obtain information on IT governance in the federal government to correctly identify what and how to audit, and to enhance the efficiency and efficacy of its actions.

In order to collect information on issues related to the procurement of IT products and services, information security, IT personnel, IT planning and the main governmental systems and databases, an encompassing survey was authorized to evaluate IT governance in the federal government.

The first survey started in 2007 and concluded in 2008. After this first edition, surveys have been conducted in even years and their findings confirmed in odd years, through audits on a sample of the surveyed agencies that usually find only few inconsistencies in the information provided by the agencies.

The survey process, as depicted in Figure 5 in the previous chapter, consists of:

1. In odd years, assessment audits based on the previous survey are executed. A sample of the agencies profiled is selected to be audited based on a risk analysis. Inputs from the previous survey such as practices adopted, agencies' budget, projects' results, and information obtained outside the survey scope are used to select the audit sample. The audits are conducted, an encompassing report is produced and individual and general recommendations are made;
 2. Based on the audits' results, mapped best practices, manager's feedback and the audit findings are used to review and improve the survey form. The required tools are arranged (survey software, communication letters are reviewed, questions review). A reviewed draft of the survey is submitted to internal and external request for comments. A timetable is approved;
 3. In even years, the survey is then conducted. The answers are provided by the agencies according the defined schedule. An individual and general report on IT governance status is produced. General conclusions about the IT Governance status of the government are drawn based on data analysis;
 4. By the end of the survey execution, all the survey process is reviewed. Improvements opportunities are registered in order to help the next cycle.
- Main products from each activity of this process are:
- Monitoring: mapping of effective benefits of IT governance improvements; mapping of major risks and deficiencies; best practices found;
 - Survey planning: improved version of survey form; timetable approved;
 - Survey execution: iGovTI (IT Governance Scoring) for each agency; feedback report analyzing the provided answers to the survey and comparative results from other similar agencies; final report on State IT governance status;
 - Survey review: improvement opportunities for the next cycle.
- In 2010, for IT Governance Survey (survey's 2nd edition) TCU created an IT Governance score named iGovTI. Although, the main goal of this score is to measure improvements in IT Governance of public sector, it has been worked as an extra stimulus

for the agencies to implement the best practices. Comments from IT administrators reveal that the control items presented in the survey are given a greater importance in their agencies and that top decision makers often benchmark overall score between agencies which leads to the setting of institutional goals over the iGovTI score improvement.

This has the advantage of clarifying what are important metrics in IT governance, helps to prioritize intermediate goals in order to improve governance and overall results, but it also has the disadvantage of pushing different agencies towards the same IT governance goals, irrespective of their particular strategies, needs or capabilities. This overemphasis on the final score of the iGovTI is currently being moderated through the release of intermediary scores that relate to different dimensions of governance and limited rankings that contain only similar agencies in a given sector, such as state-owned companies on competitive sectors, courts or administrative departments.

The effort to show best practices in IT governance and the results of our audits and surveys to public administrators has led to the publication of guides and executive summaries, as well as pedagogical actions. Examples are the publishing in

2012 of the “Guide to good practices in procurement for information technology solutions” and a technical note, in 2014, about “IT Governance Systems conception”. On the other hand, several presentations and seminars have been conducted since the first survey in 2007. The last two seminars were “International Seminar on Coordinated Audit of IT Governance”, in July of 2014, and the “Public Dialogue: IT Governance - External Control in Action”, in May of 2014.

3.5 Evolution

Some improvement signs were already detected in 2010, particularly the ones concerning the increase in the number of agencies that had institutional strategic planning and had adopted an IT career.

In 2012, it was found that half the institutions evaluated got a mid-range IT governance capacity degree, which represents a substantial increase if compared to 2010, when only 38% of the agencies were in this range. The ratio of institutions considered to be in the advanced stage has risen from 5% in 2010 to 16% in 2012. Other improvements were also observed, such as the increase in

agencies with a constituted IT committee and better oversight on IT projects by top management.

Furthermore, some of the aforementioned evolution can also be attributable to improvements in the normative regulation of some dimensions of IT governance such as IT procurement, information security and corporate governance. Part of this regulatory action was induced by SAI recommendations derived from the IT governance evaluation effort. This high level normative direction was also detailed in guides and manuals produced by regulators, for example guides were produced on how to elaborate an IT plan, constitute an IT committee, how to measure software projects or establish a software developing process etc.

3.6 Key Messages

- It is fundamental to obtain information about governmental agencies. The survey can be the sole compilation of data regarding IT governance for government agencies, but it also allows the development of metrics to evaluate IT performance. It enables following the evolution of major indicators in IT governance and testing the results of policies aimed at improving IT governance;
- The survey also indicates best practices and references in IT controls (such as COBIT) to the management universe, especially the less mature institutions. This compilation may help them to improve their practices and results;
- It creates a virtuous cycle of improvements in IT governance: evaluation of results; benchmarking among entities; recognition for best public administrators;
- Providing adequate support for the public administrators that will fill the survey is crucial: fast response to doubts, FAQ, references to legal documents and norms that support the questions etc.;
- The feedback report has a great value: non-technical language should be used so that a wide audience can easily understand the main conclusions; association of deficits in controls to their associated risks shall be made. On the other hand, comparisons of results between similar entities may induce improvements. Its information may also be used as gap analysis done at scale for the whole government.

4. AUDITOR GENERAL OF SOUTH AFRICA

“INDIVIDUAL ORGANIZATION” METHOD

4.1 Summary

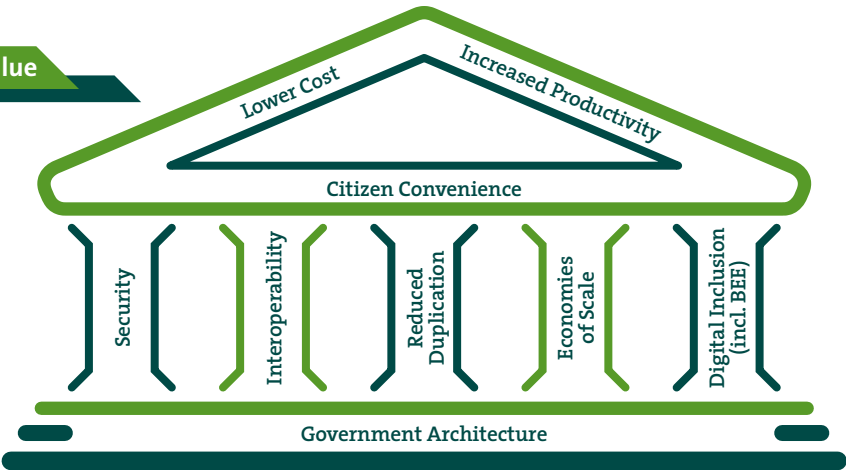
As in any organization, the effective use of information technology (IT) in government is a key success factor in its response to service demands as it enables government to leverage the agility of programs and related processes.

The important role that IT has to play in achieving government’s vision is acknowledged in the South African public service regulations, which

require all government and public sector institutions to manage IT effectively and efficiently. Figure 10 illustrates the principles of the ICT house of values adopted to provide direction in this regard.

To ensure the effective and efficient use of the IT resources allocated, the regulations stipulate that the acquisition, management and use of IT have to be informed by the principles of Batho Pele (DPSA, 2014) and King III (PwC,

Figure 10: ICT house of value

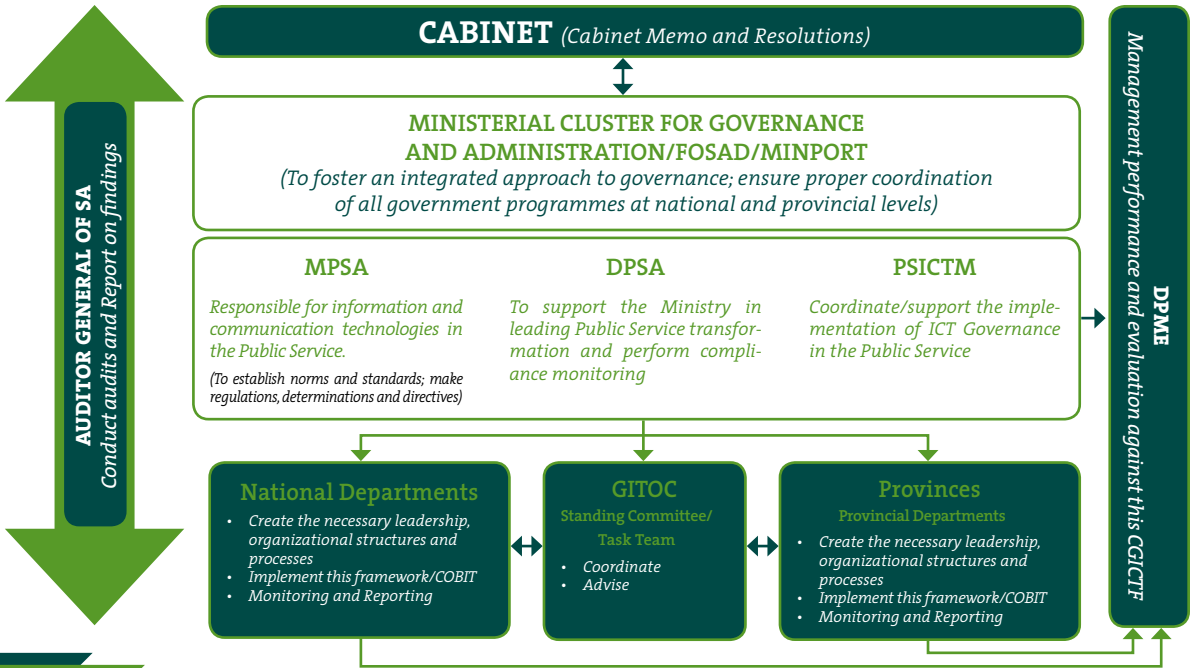


2010). In addition, those charged with governance are required by legislation to exercise due care, diligence and appropriate disclosure in the deployment of resources to programs aimed at assisting government in achieving its service delivery objectives. The Government of South Africa, through the Department of Public Service and Administration (DPSA), approved the Corporate Governance of Information and Communication Technology Policy Framework

(CGICTPF) in December 2012 (DPSA, 2013a). On a high level, the CGICTPF can be defined as a directive that assists executive management and leadership in government in establishing the key IT governance processes in their organizations. These processes involve:

- IT-related decision-making structures;
- Accountability structures for IT;
- IT governance processes;

Figure 11: Oversight structure for corporate governance of ICT in public service



- IT reporting structures;
- IT policies and standards;
- IT compliance;
- IT controls and risk mitigation.

The implementation of the CGICTPF has paid due consideration to the existing governance structures, as depicted in Figure 11.

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.

The Supreme Audit Institution of South Africa (SAI-SA) has been involved in the process since its inception and continues to do so. This ensures that we remain abreast of the developments and are aware of the intricacies and challenges that come with the implementation of the CGICTPF. The implementation of

the CGICTPF is an essential component in ensuring efficiency and security in government's business operations.

4.2 The SAI

4.2.1 Mandate and Functions

Chapter 9 of the Constitution of the Republic of South Africa, 1996, establishes the Auditor-General of South Africa as one of the state institutions supporting constitutional democracy. The Constitution recognizes the importance and guarantees the independence of the Auditor-General of South Africa (AGSA), stating that the AGSA must be impartial and must exercise its powers and perform its functions without fear, favor or prejudice.

The functions of the AGSA, as Supreme Audit Institution of South Africa, are described in section 188 of the Constitution and are further regulated in the Public Audit Act, 2004 (Act No. 25 of 2004) (PAA), which mandates the AGSA to perform constitutional and other functions. Constitutional functions are those that the AGSA performs to comply with the broader mandate described in the

Constitution. Section 4 of the PAA makes a further distinction between mandatory and discretionary audits.

4.2.2 Accountability and Reporting

The AGSA is accountable to the National Assembly in terms of section 181(5) of the Constitution and section 3(d) of the PAA and has to report on its activities and the performance of its functions in terms of section 10 of the PAA. The main accountability instruments are the AGSA's budgetary and strategic plan and its annual report, both of which are tabled annually in the National Assembly.

The Standing Committee on the Auditor-General (SCoAG), established in terms of section 10(3) of the PAA, oversees the performance of the AGSA on behalf of the National Assembly.

4.2.3 Products

The AGSA annually produces audit reports on all government departments, public entities, municipalities and public institutions. Over and above these entity-specific reports, the audit outcomes are analyzed in general reports that cover both the Public Finance Management Act

(PFMA) and Municipal Finance Management Act (MFMA) audit cycles. In addition, the AGSA also issues reports on discretionary audits, performance audits and other special audits.

The AGSA submits reports to the legislature with a direct interest in the audit, namely Parliament, provincial legislatures or municipal councils. These reports are then used in accordance with their own rules and procedures for oversight.

4.3 The Challenge

It is a well-known phenomenon that the implementation of government programs comes with various challenges. These challenges, if not addressed, may nullify the good intentions and become a drain on government resources aimed at ensuring the successful implementation of key interventions, such as implementing the CGICTPF across all spheres of government.

SAI-SA, through its Information Systems Auditing (ISA) business unit, participates in various forums that oversee and establish processes that help government to deploy and derive value from the investment made in IT.

The purpose of SAI-SA's participation in these forums is to advocate the use of best practices and to highlight proactively the risks that government departments will face in the different phases of implementing the CGICTPF.

The DPSA has moderated the implementation of phase 1 at the national and provincial departments. An assessment of the results of the phase 1 deliverables, which were mainly aimed at establishing enabling structures for the successful implementation of the CGICTPF in the environments of government entities, revealed the following challenges:

- Generally, there was a lack of understanding and application of governance principles as articulated in the CGICTPF;
- Cognizance was not always taken of the assessment standards and requirements;
- Teething challenges that related to coordination and cooperation were experienced at the provinces and some national departments;
- ICT functions were not adequately capacitated;

- Compliance and value delivery in terms of the framework were not always well understood, i.e. although the framework would go a long way in ensuring compliance, its main purpose remains to ensure value delivery.

4.4 What Was Done

During the revision of its strategy in 2008-09, SAI-SA made a decision to put measures in place to influence audit outcomes across all spheres of government. At the time, the audit results painted a bleak picture of matters relating to governance, accountability, finance, human resources and ICT. SAI-SA therefore prioritized the problem areas and put a strategy in place that focused on collaboration and more regular engagement with its stakeholders throughout the financial year, instead of only during the audits.

The development of the CGICTPF was a result of quarterly stakeholder engagements aimed at promoting a more constructive relationship with auditees and facilitating more positive audit outcomes, especially in the area of IT audit findings, which were never remedied by the executive and leadership of government departments.

4.5 Evolution

Government, through the Department of Performance Monitoring and Evaluation (DPME), has established performance measurement processes to monitor constantly the following four key management practices:

- Strategic management;
- Governance and accountability;
- Human resource management;
- Financial management.

Within the above practices there are 32 standards, which are based on existing policies and regulations (DPME, MPAT Standards 2014, 2014).

The implementation of the CGICTPF is a performance area covered under the key management practice of governance and accountability. This process is facilitated by the Management Performance Assessment Tool (MPAT). According to the MPAT standards of 2014, the quality of management practice will be assessed in three dimensions; concerning documentation of management policies, systems and frameworks, actual application of these in good management practice and the extent to which management practice in each

performance area contributes adequately to improving organizational results.

Table 4 outlines the four levels of assessment of the quality of management practice, which are used to score the performance of departments.

The DPSA is responsible for ensuring compliance with the CGICTPF and has compiled the following action list, which was informed by the moderation results of phase 1 of the implementation of the CGICTPF:

- A compliance check list, developed and aligned to the requirements of each assessment level (DPME, DPME MPAT 1.4 2.8.1 CGICT tick list);
- Annual updating of the MPAT assessment standards;
- National and provincial workshops on the CGICTPF;
- Focused engagements with the departments that require support on phase 2 deliverables;
- Collaboration with the ISA business unit of the AGSA to gain an understanding of the

- audit outcomes and to endorse the advocacy of following best practice standards;
- Expanding of the capacity of the DPSA and the moderation teams that oversee the implementation of the CGICTPF in government.

The DPSA highlighted capacity issues as a major problem in ensuring adequate oversight of the processes aimed at facilitating effective implementation of the CGICTPF.

The role of SAI-SA is to annually audit the control measures that government has put in place, such as those outlined above (AGSA).

Table 4: Assessment Levels

Level of compliance with legal/regulatory requirements (%)	Description	Response
Under 25% - level 1	A department that has insufficient capability is largely non-compliant, and is performing poorly in terms of its management practices. It is not well placed to address these weaknesses in the short to medium term and needs additional action and support to improve performance for effective delivery.	Intense support: diagnostic assessment of the causes of the problems and assistance with the development, implementation and monitoring of an improvement plan.
25%-50% - level 2	A department that has improving capability is partially compliant or improving its compliance, but is performing below expectations in terms of its management practices. There are no clear plans to improve its performance and support action is required.	Support similar to level one, but less intense.
50%-75% - level 3	A department that has sufficient capability is fully compliant and its performance is adequate in terms of management practices. It has identified its capability gaps and is well placed to address them.	Monitor.
75%-100% - level 4	A department that has excellent capability is fully compliant, and is performing above expectations. There is evidence of learning and benchmarking against global good practice, which confirms progress towards world-class standard.	Develop and disseminate case studies.

4.6 Key Messages

SAI-SA, through its engagements at the different forums, follows up and ensures that the mandates, roles and responsibilities in terms of IT governance are properly coordinated and focused on putting processes and measures in place for responding to the following key questions that the leadership in government should continue to ask:

- Are adequate processes in place to provide clarity and understanding of how IT decisions are taken and who is accountable?
- Do the executive and leadership of government departments have the appetite to adopt an IT governance framework that defines and supports decision models, governance structures, accountability and governance processes?
- Do the executive and leadership of government departments involve IT in strategic business decisions and planning?
- Do the executive and leadership of government departments understand the investment in IT and the benefits thereof?
- Are processes in place to protect adequately citizens' information, clearly delineating intellectual property and information?
- How do those charged with governance ensure compliance with IT laws, rules, codes, standards and regulations?
- Do the executive and leadership of government departments have processes to measure the value delivered by IT?
- How do the executive and leadership deal with the IT risk of their government departments?
- Is IT a regular item on the agenda of the executive and leadership structures of government?

An honest response to the above questions by the executive and leadership of government departments provides a basis for an action plan that tracks and monitors the implementation of the CGICTPF.

REFERENCES



- AGSA. (n.d.). Auditing IT Governance. Presentation at GITOC.
- Brisebois, R., Boyd, G., & Shadid, Z. (n.d.). What is IT Governance ? Retrieved from http://www.intosaiitaudit.org/intoit_articles/25_p30top35.pdf
- DPME. (2014). MPAT Standards 2014. Retrieved from <http://www.dpme.gov.za/keyfocusareas/mpatSite/Pages/default.aspx>
- DPME. (n.d.). DPME MPAT 1.4 2.8.1 CGICT tick list. Retrieved from <http://www.dpme.gov.za/keyfocusareas/mpatSite/Pages/default.aspx>
- DPSA. (2013a). Corporate Governance of ICT Policy Framework. Retrieved from http://www.dpsa.gov.za/dpsa2g/documents/psictm/2013/CGICT_Policy_Framework.pdf
- DPSA. (2013b). Directive from DPSA. Retrieved from http://www.dpsa.gov.za/dpsa2g/documents/psictm/2013/Directive_Policy_04_02_2013.pdf
- DPSA. (2014). Batho Pele Government Principles. Retrieved from http://www.dpsa.gov.za/documents/Abridged_BP_programme_July2014.pdf
- EUROSAT IT Working Group. (2007). A Methodology for IT self-assessment by SAIs, version 4.0. Retrieved from http://www.eurosai-it.org/documents/members/IT_self-assessment/itsa_guide_version_4_0.pdf
- Gisselquist, R. M. (2012). Good Governance as a Concept. Retrieved from http://www.wider.unu.edu/publications/working-papers/2012/en_GB/wp2012-030
- INTOSAI. (2014). WGITA – IDI Handbook on IT Audit for Supreme Audit Institutions.

REFERENCES

- ISACA. (2003). The COBIT Maturity Model in a Vendor Evaluation Case, Information Systems Control Journal, volume 3.
- ISACA. (2009). Implementing and Continually Improving IT Governance.
- ISACA. (2011a). COBIT Process Assessment Model (PAM): Using COBIT 4.1.
- ISACA. (2011b). COBIT Self-Assessment Guide: Using COBIT 4.1.
- ISACA. (2012a). A Business Framework for the Governance and Management of Enterprise IT.
- ISACA. (2012b). COBIT 5 Enabling Processes.
- ISACA. (2013a). COBIT Process Assessment Model (PAM): Using COBIT 5.
- ISACA. (2013b). COBIT Self-Assessment Guide: Using COBIT 5.
- ISACA. (2013c). COBIT 5 for Risk.
- ISACA. (2013d). COBIT 5 for Assurance.
- ISACA. (2014). Risk Scenarios Using COBIT 5 for Risk. Retrieved from <http://www.isaca.org/knowledge-center/research/researchdeliverables/pages/risk-scenarios-using-cobit-5-for-risk.aspx>
- ISACA. (n.d.). Audit/Assurance Programs. Retrieved from <http://www.isaca.org/Knowledge-Center/Research/Pages/Audit-Assurance-Programs.aspx>
- ISACF. (2000). COBIT 3rd Edition.

- ISO/IEC. (2008). 38500. IT Governance Standard.
- ISO/IEC. (2013). 27002. Information Security Standard.
- ITGI. (2003). Board Briefing on IT Governance. Retrieved from <http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx>
- ITGI. (2005). COBIT 4.0 Control Objectives. Management Guidelines. Maturity Models.
- ITGI. (2007). COBIT 4.1 Framework. Control Objectives. Management Guidelines. Maturity Models.
- ITGI. (2008a). Understanding How Business Goals Drive IT Goals.
- ITGI. (2008b). IT Governance and Process Maturity.
- PwC. (2010). King III in the Public Sector. Retrieved from http://cymcdn.com/sites/www.iodsa.co.za/resource/collection/c7c92b6a-029d-4f04-8750-94491a6387dc/Executive_guide_to_King_III_Public_Sector.pdf?hhSearchTerms=%22Executive+and+Guide+and+King+and+III+and+Public+and+Sector%22
- TCU. (2014). Governance Benchmark applicable to public administration agencies. Retrieved from <http://portal2.tcu.gov.br/portal/pls/portal/docs/2663788.PDF>
- The National Audit Office of Lithuania. (2014). Information Technology Strategy of the National Audit Office 2015–2020. Retrieved from http://www.vkontrolė.lt/en/docs/IT_strategy_2015_2020.pdf
- The National Computing Centre. (2005). Developing a successful governance strategy.



Responsibility for Content

Auditor-General of South Africa
Federal Court of Accounts of Brazil
National Audit Office of Lithuania
US Government Accountability Office

Design

NCE - TCU

Federal Court of Accounts of Brazil
SAFS Quadra 4 – Lote1
Edifício Sede
Phone: +55 61 3316.7256
www.tcu.gov.br

(Ombudsman)
Phone: +55 61 0800 644 1500



GET.IT
Governance Evaluation
Techniques for
Information Technology

www.tcu.gov.br

www.intosai.org