

DRAFT

CONTRALORIA GENERAL DE LA REPUBLICA DE COSTA RICA

5TH PERFORMANCE AUDITING SEMINAR

INTOSAI STANDING COMMITTEE ON IT AUDIT

MAJOR THEME: IT GOVERNANCE

**IT GOVERNANCE ISSUES IN THE INSTITUTIONS WE
HAVE AUDITED: LESSONS LEARNED**

NOVEMBER, 2006

DRAFT

CONTENTS

| | |
|--|----|
| SAI and IT Governance Oversight..... | 3 |
| Case Studies - SAI perspectives regarding IT Governance Institute Model..... | 5 |
| Conclusions | 10 |

DRAFT

SAI and IT Governance Oversight

Governance and *management* differ in nature, even though they are often considered the same concept, in practice.

For instance, *governance* refers to “*what?*” should be accomplished by exercising control, authority and direction over the organisation. It focuses and considers issues related with the long term, such as the organisational mission, values, policies, goals, objectives and strategies, but overall, it deals with accountability.

Management, from a general perspective, refers to the question “*how it does it?*”. This issue deals with the ways an organisation uses to achieve its objectives. As well, management levels are accountable, as a principle of the nature of their tasks, to the Executive Management, which also is accountable to the Board of Directors, or a similar governing body. Thus, management is responsible for exercising the organisation’s mission, values, policies, goals, objectives and strategies.

The Board of Directors, or a similar governing body, usually should provide an organisational governance framework. This governance framework comprises the high level policies and orientations to drive the enterprise alignment, direct management to deliver measurable value, manage high level risks, support organisational learning and growth, and measure performance and results. Management should comply with these directives.

This proposal refers to a specific branch of the modern governance model: the information technology (IT) governance framework.

DRAFT

Governance as a fundament for organisational administration integrates several sub themes, such as financial, operational, marketing, social impact and information technology (IT) frameworks.

In this context, IT governance refers to a responsibility that pertains to the board of directors and the executive management. According to the IT Governance Institute, it is an integral component to the whole enterprise governance and is composed of “the leadership and organisational structures and processes that ensure that the organisation’s IT sustains and extends the organisation’s strategies and objectives”.¹ IT governance consists of processes, leadership and organisational structures for the purpose of sustaining and extending the organisational strategies.

The alignment between the organisational and the IT strategies is an important requirement for a successful IT contribution for achieving enterprise objectives. Due alignment of activities should facilitate the general enterprise strategies to be tailored into the IT strategy. In the next level, alignment should provide for support of business operations with IT operations.

Another important issue relates with the organisation’s strategic objectives. The IT strategic objectives should comply with the proper business alignment in order to support the general organisation objectives. In order to exercise the enterprise strategy and its business functions, IT should provide a set of drivers like application architecture, technical infrastructure, staffing and resources sourcing, all adequately funded by the proper resources.

IT governance provides a framework. As a basis, the framework requires well established objectives to ensure that IT aligns with the business, enables and maximises

¹ IT Governance Institute. Board Briefing on IT Governance.

DRAFT

benefits, responsibly uses resources, and has a sound risk management process. By comparing the objectives against IT activities, such as increasing automation (creating effectiveness), decreasing costs (providing efficiency) and managing risks (assuring security, compliance and reliability), the framework helps in providing direction and measuring performance as to the achievement of the objectives.

As well, IT governance has several focus areas, according to the IT Governance Institute. Two of these areas relate to outcomes: value delivery and risk management. The other three areas propose drivers: strategic alignment, resource management and performance measurement. Upon the regular application of oversight functions, the areas enter a cycle that permits the accomplishment of objectives.

IT Governance is also driven and comprises a process. Based on defined stakeholders' value drivers, the IT governance process steers the IT strategy, which as well directs the IT process to obtain and measure the usage of resources to execute the related tasks and responsibilities. By exercising oversight over results, outcomes, performance, risks and asset management, the It governance process can help improving the IT processes and confirming or challenging the strategy.

Case Studies - SAI perspectives regarding IT Governance Institute

Model

The IT Governance Institute model comprises five components:

- Alignment
- Value Added

DRAFT

- Risk Management
- Resource Management
- Performance Monitoring.

Related with the IT governance model already mentioned in this paper, the Costa Rican SAI has built up some experience over IT oversight. IT is one of the most important investments in the government operations; thus, is one of the oversight priorities for our SAI.

In an important degree, we have covered those five IT governance components during several years of exercising oversight over the government's IT investments and operations. Our area of expertise has focused on the organisational and IT alignment, risk management and performance monitoring. The value added process and resource management have also been included in some degree in our examinations and results.

Our experiences in IT audits and evaluations has been challenged by the application of several IT control standards; some in-house designed and other were taken as reference from general accepted IT control and management models. Far from just dealing with technical, low level IT decisions, the usage of these standards as criteria for our studies has fostered three main high level governance and management edges:

1. Governance integration
2. Roles and responsibilities
3. Implementation strategies.

As a result, our office has developed several reports, as result of auditing processes and areas related with:

DRAFT

- Immigration Systems
- Land Registry Systems
- Civil Registry Systems
- Social Insurance Systems
- Customs Systems
- Public Education Payroll Systems
- Treasury Board Systems
- Telecommunications Systems

Following, we will present a matrix of the most important findings observed during those audits, in association with IT Governance issues.

DRAFT

| SYSTEM/ FINDING | IT GOVERNANCE ISSUE | | | | |
|---|--|--|---|---|---|
| | ALIGNMENT | VALUE ADDED | RISK MANAGEMENT | RESOURCE MANAGEMENT | PERFORMANCE MONITORING |
| IMMIGRATION | | | | | |
| Poor strategic planning | Missing points of reference to setup governance (north) | | | | |
| Structure weaknesses | | | | Lack of capacity | Lack of clarity on who is responsible for what |
| Inexistence of IT Audit | Missing an essential part of accountability framework. Advise and independent opinion to the Board. | | | | |
| Deviations from confidentiality criteria | Confidentiality is the very nature of this system | IT should leverage the core business | Privacy issues | | |
| Service unavailability | | IT should facilitate high availability | National security Loss of confidence Legal consequences | Service level agreements | |
| Weak controls in branch offices | Importance of organizational integrity | | Damage to public image | | Poor inputs for accountability |
| | | | | | |
| LAND REGISTRY | | | | | |
| Poor IT Infrastructure Management | Strategic plans out of date | | High dependence on single contractor | High cost of acquisition | |
| Lack of risk management | Missing the cornerstone for the accountability framework. Threats and vulnerabilities not desirable combination for legal assurance. | | | | |
| Absence of performance management | | | | | Lack of ability to set preventive actions on major deviations |
| Information security weaknesses | Lack of mature policies | | Threat to availability, continuity and performance | Incomplete business contingency plan | |
| People management | | Not the best scenario for innovation | | Insufficient training | Results poorer than expected |
| Inexistence of IT Audit | Missing an essential part of accountability framework. Advise and independent opinion to the Board. | | | | |
| CIVIL REGISTRY | | | | | |
| Inexistence of business / IT strategic planning processes | Missing points of reference to setup governance (north) | | | | |
| Absence of feasibility studies for complex projects | | Major gap between expectations and reality | Unknowable high risks involved Projects are usually over | Lack of internal capacity to deal with complex projects | High dependence on single and dominant contractor |

DRAFT

| SYSTEM / FINDING | IT GOVERNANCE ISSUE | | | | |
|--|---|--|--|---|--|
| | ALIGNMENT | VALUE ADDED | RISK MANAGEMENT | RESOURCE MANAGEMENT | PERFORMANCE MONITORING |
| | | | dimensioned | | |
| Business continuity plans not in place | | IT should contribute to ongoing service | Not responsiveness Legal consequences | | |
| Absence of project cost management | | | | Unknowable type and cost of resources involved | Unknowable real amount of investments |
| SOCIAL INSURANCE | | | | | |
| Absence of risk management process | Missing the cornerstone for the accountability framework. Threats and vulnerabilities not desirable combination for national public health. | | | | |
| IT hierarchical level | | IT function has no overall impact in core business | IT not responding to business as a whole | Few resources to leverage IT function | IT not in good position to be held as accountable for. |
| Board of directors not involved | Missing the "raison d'etre" of governance model. Poor commitment and weak control environment | | | | |
| PUBLIC EDUCATION PAYROLL | | | | | |
| Poor project management | | Expectations not accomplished Processes falling back | High monetary losses Unsatisfied clients | Failed project Project went over spent and delayed | Not clarity on who was responsible between Administration and contractor |
| TREASURY BOARD | | | | | |
| Weak EFT solution and procedures | | | Wrong doing and fraud | Misappropriation of public resources | Weaknesses on internal control Not feasible to follow the dollar |
| CUSTOMS | | | | | |
| Poor project management | | | Over costing Significant delays Not compliance | Poor infrastructure Over budgeting | |
| TELECOMMUNICATIONS | | | | | |
| Evolution of legacy applications | No integration between Corporation and IT long term planning | Internal clients never bought the idea Entity remains behind best practices | High monetary risk Few chances for success | High cost of opportunity involved | Board absent of technical and business argumentation |

Conclusions

DRAFT

Throughout our experience on IT auditing during the last few years, we have noticed that Boards are usually absent in planning, developing and monitoring major IT initiatives. As well we have seen several failed projects, poor project management experiences, heavy monetary losses, high and inconvenient dependence on certain dominant vendors, among other dysfunctions.

As a matter of fact, Costa Rica's government difficulties on IT governance issues has gone so far, that even the national legislative body issued a special report and several regulations that pertains specifically to risks mitigation on IT contracting.

We believe, in order to avoid those negative effects and move the yard sticks forward, the entities should consider the following guidance:

Do's

- Promote and adopt international IT governance standards and best practices
- Foster participation of the Board of Directors in setting the stage
- Build capacity on IT governance at all levels
- Assure IT enterprise alignment
- Improve objectives setting at strategic, tactic and operational levels (SMART philosophy)
- Encourage a performance management and monitoring processes

DRAFT

- Improve IT project and risks management
- Include IT procurement in corporative fraud preventive processes
- Document and share experiences (good and bad) among public sector

Don'ts

- Ignore the Board of Directors
- Leave the IT technical staff alone
- Leave aside an accountability framework
- Define poor and not measurable objectives
- Launch huge project without proper internal capacity
- Leave aside best practices
- Ignore IT audit findings and recommendations

REFERENCES

- www.cgr.go.cr Studies: Dirección General de Migración, Registro Público, Caja del Seguro Social, Dirección General de Aduanas, Ministerio de Educación, Ministerio de Hacienda.