

DRAFT

Introduction to the Seminar:

What Is IT Governance and Why Is It Important?

Richard Brisebois, Greg Boyd , and Ziad Shadid, Office of the Auditor General of Canada

Information technology (IT) governance, although sometimes mistaken for an independent field of study, is actually part of an organization's strategies for corporate governance--the processes, customs, policies, laws, management practices, and institutions affecting the way a corporation (that is, any organization, such as a business) is controlled and managed. These strategies--including all the relationships among the many stakeholders involved—are aimed at enabling the organization to meet its objectives in the most effective and efficient manner possible. Such strategies include the participation of all stakeholders in decision making; balancing risks and rewards; implementing best practises, such as performance metrics; using IT auditors; as well as meeting obstacles.

Areas and Effective Strategy for Corporate Governance

Corporate governance includes several areas:

- **Accountability and fiduciary duty:** The implementation of guidelines and mechanisms to ensure management acts in good faith and that the public sector organization is protected from wrongdoing or fraud.
- **Economic efficiency perspective:** How corporate governance system aims to optimize results and meet objectives.
- **Strategic efficiency perspective:** Public policy objectives--such as alleviation of poverty, access to markets, income stabilization, health care, and job creation--which are the main focus of most public sector institutions, but are not readily measured in economic terms.
- **Stakeholder perspective:** Focuses attention on accountability from stakeholders such as citizens, employees, businesses, and different levels of government (that is, provincial [state], municipal, or other local authorities.)

IT governance should never be seen as a discipline on its own, but as a means to fit IT projects into the organization's strategies for corporate governance. One effective strategy for corporate governance allows an organization to manage all aspects of its activities necessary to meet its objectives. As part of this strategy, all stakeholders are

DRAFT

required to participate in the decision-making process. Such participation creates a shared acceptance of responsibility for critical systems and ensures that IT-related decisions are made and driven by the organization and not vice versa.

IT Governance—What Is It, Why Needed, and What Are Best Practises

The following defines and explains IT governance:

What IT IS

IT governance has been defined in various ways by different people. However, it is generally recognized to include management oversight, processes and rules for conducting various activities and a measurement and reporting mechanism of status and quality. Examples of how people have defined IT Governance include:

- **[according to whom?]**¹ Rules and processes that enable effective functioning, including the recognition and management of risks.
- Paul Williams:² The structure, oversight, and management processes that ensure, in a controlled way, the (1) delivery of the expected benefits of IT and (2) the enhancement of the long-term success of the project.
- Board Briefing on IT Governance:³ The board of directors and senior management consisting of the leadership, structures, and processes that ensure that the organization's IT sustains and extends its strategies and objectives.
- COBIT:⁴ A structure of relationships and processes to direct and control the organization, by adding value while balancing risk versus return over IT and its processes, in order to achieve its objectives.
- Robert Roussey:⁵ How senior managers consider IT in their supervision, monitoring, control, and direction of the organization and the immense impact IT will on whether the organization will realize its objectives.

¹ [?][footnotes need to be completed]

² [?]

³ 2nd edition, IT Governance Institute[?]

⁴ July 2000[?]

⁵ University of Southern California[?]

DRAFT

- Michael Cangemi:⁶ Applying to IT the same the level of commitment applied to corporate governance.
- Board Briefing on IT Governance:⁷ (1) Delivery of value to the organization, driven by strategic alignment of IT with the organization’s objectives, and (2) mitigation of IT risks, by embedding accountability into the project; both supported by adequate resources and measured to ensure that the desired results are obtained.

Why IT Is Needed

IT governance is needed to ensure that the investments in IT (1) generate value—reward—and (2) mitigate IT-associated risks, avoiding failure. IT is central to organizational success--effective and efficient delivery of services and goods--especially when the IT is designed to bring about change in an organization. This change process, commonly referred to as “business transformation,” is now the prime enabler of new business models both in the private and public sectors. Business transformation offers many rewards, but it also has the potential for many risks, which may disrupt operations and have unintended consequences. The dilemma becomes how to balance risk and rewards in using IT to enable organizational change.

What the Best Practises Are

Despite efforts of the software industry to identify and adopt best practices in the development of IT projects, there is still a high rate of failure and missed objectives. Most IT projects do not meet the organization’s objectives. For example, in the Standish Group’s Chaos biennial survey of IT projects over the last 10 years, the success and failure trends of approximately 50,000 IT projects were analyzed. In a 2004 report the group concluded, “29% of projects succeeded (delivered on time, on budget, with required features and functions); 53% are challenged (late, over budget and/or with less than the required features and functions; and 18% have failed (cancelled prior to completion or delivered and never used).”

A key best practise is implementing an organizational structure, including an effective governance framework, with well-defined roles and responsibilities for IT, related processes, and IT auditors. Such a framework ensures that IT investments are aligned and delivered in accordance with corporate objectives and strategies; without this framework, IT projects are more susceptible to failure. But many organizations fail to consider the importance of IT governance. They take on IT projects without fully understanding what

⁶ President and COO, Etienne Aigner Group Inc. [?]

⁷ 2nd edition, IT Governance Institute[?]

the organization's requirements are for the project and how this project links to the organization's objectives.

Identifying organizational objectives is another key best practise for IT governance. Historically, senior managers saw IT projects from the limited perspective of input and output objectives. This inefficient and ineffective perspective stemmed directly from these managers' lack of technical experience to deal with the complexity of such projects. In addition, these managers were unjustly blamed for the vast inefficiencies caused by the organization's failure to integrate the objectives of IT projects with the overall objectives of the organization.

Finally, without effective governance, IT projects have a higher risk of failure. For success, the organization should consider all of the following factors, which lead to best practises: high-level framework, independent assurance, performance management reporting, resource management, risk management, strategic alignment, and value delivery:

- High-level framework—including defining leadership, processes, roles and responsibilities, information requirements, and organizational structures—ensures the IT investment is aligned with the overall strategies of the organization, maximizing the application of available IT opportunities.
- 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 managers are provided with a fair assessment of the IT project being audited.
- Resource management, through regular assessments, ensures that IT has sufficient, competent, and efficient resources to meet the organization's demands.
- Risk management, through embedding in the responsibilities of the organization, ensures that the organization and IT regularly assess and report IT-related risks and organizational impact. Exposures of any problems are followed up, with special attention paid to any potential negative effects on the overall objectives of the organization.
- Strategic alignment—a shared understanding between the organization's management and the IT department—(1) enables the board and senior management to understand strategic IT issues, such as the role of IT, as well as technology insights and capabilities and (2) ensures that the IT investment is aligned with the overall strategies of the organization, maximizing the use of available IT opportunities.

DRAFT

- Value delivery optimizes the benefits that can be achieved from each IT investment. Such investment should always provide value to the organization and be driven by the needs of the investing entity.
- Performance management reporting--including accurate, timely, and relevant portfolio, program, and IT project reports to senior management--provides a thorough review of the progress being made towards the identified objectives of the IT project. Through this review, the organization can assess IT performance--which of the planned objectives have been achieved, which deliverables have been obtained, and what shortfalls need to be addressed. Performance metrics is a good way to get some of the data needed for performance.

The Importance of Performance Metrics for IT Governance

Performance metrics is the basis for sound and rigorous IT governance. In order for an organization to have such governance, it must be able to see where true value is being added to its IT projects. Having a well-defined set of performance metrics provides management with the means to measure success and determine what areas need to be focused on, thus improving the effectiveness and efficiency of IT projects. Organizations that clearly define and apply these metrics to IT are able to quantitatively validate the success of their IT investments. Without performance metrics to back one up, it would be difficult to gauge the progress that IT projects are making towards achieving IT objectives. Best guesses are all that could be provided. The benefits of performance metrics include

- improvement in the quality of IT services over time,
- reduction in IT risks over time,
- enhanced delivery, and
- reduction in costs of delivering IT services over time.

There are two types of performance metrics: (1) metrics that are used to measure the performance of IT projects in development and (2) metrics that are used to measure the success of ongoing or repetitive IT services. For (1), a prescribed set of measurements are used to track project development and allow an organization to measure the progress of a project at all stages of the life cycle. For (2), generally, there are variations for each organization and the types of IT services it uses.

One would never be able to list all the different metrics used to measure IT effectively, but the following metrics are common to most organizations and, depending on when and where one collects the data, can be used for both project development and services:

- IT costs by category and by activity: The organization can see the amount invested in each activity and determine the value added by the financial investment involved.

DRAFT

- IT staff numbers and costs analyzed by activity: The organization can measure the value added to each activity compared with the amount of resources committed to it.
- Outsourcing ratios: The organization can determine the effectiveness of its own staff and allow them to gauge their reliance on external resources.
- IT-related operational risk incidents (number and value): The organization can measure how well risk is being handled by identifying risks, their mitigation, and the cost of failing to mitigate them; these measurements should then be brought to the attention of management.

Other examples of some common metrics include full-time versus contract IT staff, workstation costs, IT-related operational risk incidents (number and value), IT-security incidents (number and value), various metrics for IT projects, and IT investment management capability maturity model (CMM) level (current and projected).

How IT Auditors Can Use Performance Metrics, Agendas, and Strategies

To make IT governance effective, IT auditors can use performance metrics, agendas, and strategies.

Performance Metrics

IT auditors can contribute to performance metrics: (1) analysis, including what the metrics mean, what the implications are, and what actions are recommended, (2) assurance on the reliability of metrics used and reported, and (3) help identify metrics. For (1), auditors can assist in the analysis of metrics reported by providing independent corroborating information on the causes of observed metrics and the effectiveness of the planned actions to correct variances. For (2), auditors can provide independent assurance about the accuracy and completeness of performance metrics by periodic assessments of the metrics reported to the organization's corporate governance. For (3), auditors can use their skills to identify performance criteria for using metrics to measure program performance. Auditors can, therefore, assist the organization in accurately collecting, reporting, and analyzing the metrics in order to inform corporate governance on results achieved.

Agendas

IT auditors can ensure IT governance is on the agenda of the (1) Supreme Audit Institutions (SAI) and (2) organization's audit committee. For (1), auditors can use historical research studies and audits completed by other SAIs to highlight the scope and objectives that can be achieved in an audit of IT governance in the organization. They can also promote IT governance as an audit domain that needs to be examined within the organization. For (2), auditors can inform the organization about IT performance and

risks, as well as brief the organization's audit committee on the importance of an independent audit review of IT governance.

Strategies

IT auditors can promote the strategies of IT governance: to (1) ask the right questions so as to ensure that management is informed about the problems, risks, and rewards that arise from the use of IT and (2) help bridge the communication gap between the organization and the IT department. For (1), auditors can ensure that an organization's IT delivers business value. This means fast, secure, and quality systems that generate a return on investment (ROI) that makes the organization's programs more efficient and effective. For (2), auditors can bring together the IT developers and IT users within an organization. To achieve the organization's objectives, the developers and users can arrive at a common understanding of the risks, as well as obstacles, they face and how to move forward in a coordinated plan of action.

Obstacles to IT Governance

Organizations should give adequate consideration to the obstacles--direct threats to the achievement of IT objectives--they face in trying to implement an effective IT governance structure. Without governance that deals with obstacles, IT will have a higher risk of failure.

Each organization faces its own unique obstacles. For each organization, environmental, political, geographical, economic, and social issues differ. Any one of these issues can create obstacles to providing effective governance. One would never be able to list all the obstacles relating to IT governance, but those common to most organizations include these: lack of project ownership, lack of senior management collaboration, poor resource management, poor risk management, and poor strategic alignment:

- **Lack of project ownership:** In the past, many IT projects were left solely in the hands of the IT department and senior management tended to steer clear of taking ownership for such projects, not giving the department a sense **[meaning here?]** of the project. Such lack of ownership led the department to (1) put the IT project at risk of failing to integrate the IT objectives with the overall objectives of the organization, creating vast inefficiencies, for which IT managers were usually blamed or (2) ignore the project.
- **Lack of senior management collaboration:** Senior management tends to be unwilling to collaborate with the IT department in the decision-making process. But management needs to be involved in such collaboration when considering major IT investments. Such collaboration ensures that management is provided with the knowledge and feedback necessary to make appropriate decisions.

DRAFT

- **Poor resource management:** To achieve optimum results at minimum costs, an organisation must manage its IT resources effectively and efficiently. Making sure that there are enough technical, hardware, software, and, most important, human resources available to deliver IT services is key to achieving value from investments in IT.
- **Poor risk management:** Poor risk management is a major obstacle to the success of most IT projects. Risk management involves assessing all potential obstacles and mitigating them. If these obstacles are not addressed at the onset of the project and throughout, the risk of failure is extremely high. Often, IT risks are those that are not well understood by senior management.
- **Poor strategic alignment:** Little or no business value may be derived from major IT investments that are not strategically aligned with the organization's objectives and resources. Such poor strategic alignment means that the IT does not necessarily contribute to the achievement of the organization's objectives.