What is IT Governance?
and why is it important for the IS auditor

BY **RICHARD BRISEBOIS**, PRINCIPAL OF IT AUDIT SERVICES, **GREG BOYD**, DIRECTOR AND **ZIAD SHADID**, AUDITOR. FROM THE OFFICE OF THE AUDITOR GENERAL OF CANADA

Introduction

In Canada and in most countries, IT governance is a common theme at IT conferences and seminars. In most cases, IT governance has been discussed from a private sector perspective. This article aims to bridge the gap between private and public sector concepts and approaches.

Corporate Governance vs. IT Governance

Corporate governance is the set of processes, customs, policies, laws, management practices and institutions affecting the way an entity is controlled and managed. It incorporates all the relationships among the many stakeholders involved and aims to organise them to meet the goals of the organisation in the most effective and efficient manner possible. An effective corporate governance strategy allows an organisation to manage all aspects of its business in order to meet its objectives.

Information technology governance, however, is a subset discipline of Corporate Governance. Although it is sometimes mistaken as a field of study on its own, IT Governance is actually a part of the overall Corporate Governance Strategy of an organisation.

Corporate Governance

The field of Corporate Governance is a multi-faceted subject that includes several fields of study. These fields include areas such as:

1. Accountability and fiduciary duty. These advocate the implementation of guidelines and mechanisms to ensure management acts in good faith and that the public organisation is protected from wrongdoing or fraud.

2. Economic efficiency view. This involves how the corporate governance system intends to optimise results, and meet its objectives.

3. Strategic efficiency view. This involves public policy objectives that are not directly measurable in economic terms such as alleviation of poverty, access to markets, income stabilisation, health care and job creation. These are issues that are the main focus of most public sector institutions and are not readily measured in economic terms.

4. Stakeholder view. This area of study focuses more attention and accountability on other stakeholders such as citizens, employees, businesses and other levels of government (i.e. provincial, municipal or local authorities).

IT Governance

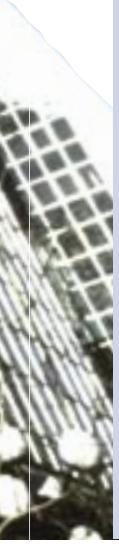
IT Governance focuses specifically on information technology systems, their performance and risk management.

The primary goals of IT Governance are to assure that the investments in IT generate business value, and to mitigate the risks that are associated with IT. This can be done by implementing an organisational structure with well-defined roles for the responsibility of information, business processes, applications and infrastructure.

IT governance should be viewed as how IT creates value that fits into the overall Corporate Governance Strategy of the organisation, 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 vice versa.

Various Definitions of IT Governance

- The structure, oversight and management processes which ensure the delivery of the expected benefits of IT in a controlled way to help enhance the long term sustainable success of the enterprise.
- IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organisational structures and processes that ensure that the organisation's IT sustains and extends the organisation's strategies and objectives.
- A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes.
- Specifying the decision rights and accountability framework to encourage desirable behaviours in the use of IT.
- Governance is not about what decisions get made – that is management – but it is about who makes the decisions and how they are made.
- 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 will have an immense impact on whether the entity will attain its vision, mission or strategic goals.



Why IT Governance is Necessary

IT governance is needed to ensure that the investments in IT generate value-reward-and mitigate IT-associated risks, avoiding failure.

IT is central to organisational success – effective and efficient delivery of services and goods – especially when the IT is designed to bring about change in an organisation. 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 when using IT to enable organisational change.

IT Governance Best Practices

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 organisation's objectives – See summary of survey carried out by the Standish Group.

Standish Group's Chaos Survey

The Standish Group's Chaos biennial survey of IT projects over the last 10 years, has analysed the success and failure trends of approximately 50,000 IT projects. 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 practice is implementing an organisational structure, including an effective governance framework, with well-defined roles and responsibilities for IT stakeholders including IS 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 organisations fail to consider the importance of IT governance. They take on IT projects without fully understanding what the organisation's requirements are for the project and how this project links to the organisation's objectives.

Identifying organisational objectives for IT is another key best practice 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 organisation's failure to integrate the objectives of IT projects with the overall objectives of the organisation.

To be successful an organisation should consider all of the following factors, which lead to best practices: 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 organisational structures – ensures the IT investment is aligned with the overall strategies of the organisation, maximising 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 organisation'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 organisation's demands.
- Risk management embedded in the responsibilities of the organisation, ensures that the organisation and IT regularly assess and report IT-related risks and organisational impact. Exposures of any problems are followed up, with special attention paid to any potential negative effects on the overall objectives of the organisation.
- Strategic alignment – a shared understanding between the organisation's management and the IT department, enables the board and senior management to understand strategic IT issues. IT strategy demonstrates the organisation's technology insights and capabilities and ensures that the IT investment is aligned with the overall strategies of the organisation, maximising the use of available IT opportunities.
- Value delivery demonstrates the benefits that can be achieved from each IT investment. Such investment should always provide value to the organisation and be driven by the needs of the investing entity.
- Performance management reporting, including accurate, timely, and relevant portfolio, programme, 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 organisation can assess IT performance in terms of 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 organisation to have good 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 in order to improve the effectiveness and efficiency of IT projects. Without performance metrics to back one up, it would be difficult to gauge the progress that IT projects are making towards achieving IT objectives. 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) development metrics that are used to measure the performance of IT projects in development and (2) services metrics that are used to measure the success of ongoing or repetitive IT services.

For development performance metrics, a prescribed set of measurements are used to track project development and allow an organisation to measure the progress of a project at all stages of the life cycle. For service metrics, generally, IT service costs are assigned to the programme based on a measure of the IT services activity used by the programme.

One would never be able to list all the different metrics used to measure IT effectively, but the following metrics are common to most organisations 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 organisation can see the amount invested in each activity and determine the value added by the financial investment involved.
- IT staff numbers and costs analysed by activity. The organisation can measure the value added of each activity compared with the amount of resources committed.
- Outsourcing ratios. The organisation 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 organisation 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).

What Can Information Systems (IS) Auditors do to make IT Governance effective?

In order to assist in the development of effective IT governance, IS auditors must:

1. Contribute to performance metrics
2. Ensure IT Governance is on the Agenda
3. Promote IT Governance strategies.

Contribute to Performance Metrics

IS auditors can contribute to performance metrics by assisting the organisation in accurately collecting reporting and analysing the metrics in order to inform corporate governance on results achieved:

- IS auditors can assist in IT performance metrics analysis, including what the metrics mean, what the implications are, and what actions are recommended. IS auditors can also provide advice by providing independent corroborating information on the causes of observed metrics and the effectiveness of the planned actions to correct variances.
- IS auditors can provide independent assurance about the accuracy and completeness of performance metrics by periodic assessments of the metrics reported to the organisation's corporate governance.
- IS auditors can use their skills to identify performance criteria for using metrics to measure programme performance.

Ensure IT Governance is on the Agenda

IS auditors can ensure IT governance is on the agenda of the Supreme Audit Institution (SAI) and the organisation's audit committee.

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 organisation. They can also promote IT governance as an audit domain that needs to be examined within the organisation.

IS auditors can also inform the organisation about IT performance and risks, as well as brief the organisation's audit committee on the importance of an independent audit review of IT governance.

Promote IT Governance Strategies

IS auditors can promote the strategies of IT governance: to 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 help bridge the communication gap between the organisation and the IT department.

Auditors can ensure that an organisation's IT delivers business value. This means fast, secure, and quality systems that generate a return on investment (ROI) that makes the organisation's programmes more efficient and effective. Auditors can also bring together the IT developers and IT users within an organisation. To achieve the organisation'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.

IT Governance Constraints

There are many constraints that face organisations that are trying to implement an effective Governance structure, particularly when there are significant IT investments involved. Without effective governance to deal with these constraints, IT projects will have a higher risk of failure.

Each organisation faces its own unique challenges as their individual environmental, political, geographical, economic and social issues differ. Any one of these issues can present obstacles to providing effective governance.

One would never be able to list all the inhibitors relating to IT Governance but the following are common to most organisations:

"There are many constraints that face organisations that are trying to implement an effective Governance structure"

Senior Management not Engaging IT

A major issue that inhibits the success of IT projects is that senior management tend to be unwilling to involve IT in the decision making process. Management needs to work with their IT department when considering major IT investments to ensure that they are provided with the knowledge and feedback necessary to make appropriate decisions.

Poor Strategic Alignment

Little or no business value may be derived from major IT investments that are not strategically aligned with the organisation's objectives and resources. Such poor strategic alignment means that IT may not be efficiently and effectively contributing to the achievement of the organisation's objectives.

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. A lack of clear leadership from senior management puts the IT project at risk of failing to integrate its objectives with the overall objectives of the organisation. Often management "passes the buck" on to the IT department, leading to a lack of integration and alignment of IT with the overall objectives of the organisation. This creates vast inefficiencies, for which IT managers are usually blamed.

Poor Risk Management

Poor risk management is a major constraint to the success of most IT projects. Risk management involves assessing all potential threats to the project and mitigating them. If these issues are not addressed at the onset of the project and throughout, the risk of failure is extremely high. Often, the most damaging IT risks are those that are not well understood by senior management.

Ineffective 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 importantly human resources available to deliver IT services is key to achieving value from investments in IT.

Conclusion

In summary, IT is an integral part of the public sector programme delivery. IT governance is an integral part of corporate governance. IT governance ensures that IT goals are met and IT risks are mitigated such that IT delivers value to sustain and grow the organisation. IT governeance drives strategic alignment between IT investment and programme delivery and must judiciously measure performance.