Monthly Newsletter

Risk Advisory

Saturday, 9 November 2019

Volume 5, Issue 7

Maximizing Business Value Through IT Governance

Use IT To Drive Performance:

A maxim "Anything that is measured, is done" can be applied to IT Governance as well. In the absence of KPIs, IT Governance may remain an initiative which does not achieve its full potential. To attain a higher maturity level in IT Governance, performance measures should be based on targets derived from the IT function's objectives. Performance measurement systems should do the following-

- Focus on customers to increase customer satisfaction
- Improve processes so that problems are anticipated and prevented
- Identify the IT costs to reduce and optimise them
- Set realistic benchmarks for comparison

Performance can be measured as a mix of objective and subjective measures. A balance scorecard approach, if used, can cover financials, customer, internal and learning dimensions. These should be easy to comprehend and interpret and can be consolidated for hierarchical reporting. Ideally, KPIs that are limited in number and focused on measures should be prioritised to support decision making.->

Better Manage Risk!:

Assessment of the current state of IT Governance, GAP analysis to identify areas for improvement and an actionable Risk Mitigation plan assist organisations in strengthening IT Governance. Critical business processes are often automated today. Management relies on the information generated by IT systems from the maze of a company's dynamic data on business operations. Thus, the decision-making process of the management depends on data and in turn on IT Systems. Similarly, direct interfaces of an organisation with its suppliers and customers depends on prevailing IT systems. Hence, there is an increasing need for effective and efficient management of IT resources, prevention of IT failures and avoidance of poor performance. The need of the hour is that IT resources be used as efficiently as possible and in an organised manner to facilitate new IT creation. ->

Framework For Successful Implementation Of IT Governance

Globally recommended best practices have a three-pronged approach to address various organisational and process issues during the course of IT Governance implementation-

- Adopt an enterprise wide approach - business and IT should define the control requirements, IT should develop a customised control model applicable to all business units and a committee approach should be used for setting and implanting directions and policies
- Top level commitment and clear accountability – without the top management's mandate, IT Governance cannot succeed and it will fail should the there be no accountability between the business and the IT function
- An agreed IT Governance and control framework - stakeholder approval should be obtained to clarify the scope of IT Governance. ->

Case Study In Context:

Higher maturity level of IT Governance provides greater assurance of not only better governance but also efficient and effective use of IT infrastructure and resources. The journey of implementation of IT Governance and improvement in the same can be understood with reference a case study of IT Governance at Ecopetrol S.A. Ecopetrol chose to implement 28 COBIT processes, giving priority to the control objectives that support Sarbanes-Oxley compliance. With the integration of the IT Management System, supported by the implementation of COBIT and the structuring of the sustainability and process-based optimization model, Ecopetrol S.A., Columbia, has laid a strong foundation for the consolidation of IT governance, risk and compliance. The Information Technology Division developed an internal exercise to determine the maturity level of these processes. After concluding that they were at an average maturity level of 2, the team identified the gaps and set up action plans to reach level 3 for the most critical processes. ->

Better Manage Risk!

Assessment of the current state of IT Governance in imperative and it includes GAP analysis to identify areas for improvement and an actionable Risk Mitigation plan assist organisations in strengthening IT Governance. Critical business processes are often automated today. Management relies on the information generated by IT systems from the maze of a company's dynamic data on business operations. Thus, the decision-making process of the management depends on data and in turn on IT Systems. Similarly, direct interfaces of an organisation with its suppliers and customers depends on prevailing IT systems. Hence, there is an increasing need for effective and efficient management of IT resources, prevention of IT failures and avoidance of poor performance. The need of the hour is that IT resources be used as efficiently as possible and in an organised manner to facilitate new IT creation.

According to Gartner Inc, IT spending is projected at a total of $3.8 trillion in 2019. However, organisations are still facing challenges that adversely affect business operations and prevent realising the full value of IT investments because of the following challenges:

- Availability, security and continuity of IT Services
- Costs and measurable return on investments
- Quality and reliability of services to avoid mishaps whilst dealing with internal and external stakeholders
- IT services not in alignment with business requirements
- Non-identification of risks to the business and corresponding mitigation plan
- Longer turnaround time to mitigate risks

Although, IT Governance is not mandatory in India, companies that have implemented Corporate Governance are better equipped to deal with IT risks which can hamper the business operations. On the contrary, the companies which failed to strengthen IT Governance continue to face the challenges which disrupt the business operations.

Corporates and governments cannot realise the full value of the IT investment if Information Technology with business strategies are not aligned and major risks are not identified and mitigated. IT governance covers these aspects. The importance of IT governance continues to grow in light of corporate scandals and failures.

Companies which implement IT governance effectively are aware of all IT related risks that have an adverse impact on their organisations. This helps improve the IT management processes to manage risks. Companies aim at ensuring that relationships with suppliers, service providers and customers are manageable. Consequently, a transparent and understandable communication of the IT activities and management processes is defined to satisfy the board and other stakeholders.

Enterprise risk comes in many forms and not only as financial risk. Regulators are concerned about operational and systemic risk, within which technology risk and information security issues are pertinent. Infrastructure protection initiatives in the US and the UK point to the sheer dependence of all enterprises on IT infrastructures and their vulnerability to new technology risks.

Ascertaining that there is transparency of the significant risks to the enterprise and clarifying the risk-taking or risk-avoidance policies of the enterprise is imperative. Being aware of the final responsibility for risk management rests with the board and hence whilst delegating to executive management, ensuring that the constraints of that delegation are effectively communicated. It's important to be conscious about the system of internal controls that have been put in place to manage risks as these controls often have the capacity to generate cost-efficiency.

A transparent and proactive risk management approach can create a competitive advantage. Embedding risk management in the operations of the enterprise, helps respond quickly to changing risks and helps report in a timely manner to the relevant levels of management that are supported by the agreed principles of escalation (what, when, where and how to report).

For IT to be effectively governed, the top managements of leading companies recognise IT risks and ensure that significant risks are mitigated. Significance of an IT risk is based on the combination of impact (what effect would the organization have on the occurrence of the risk) and the likelihood (the probability of the risk occurring). The complexity and dynamic nature of the IT environment calls for education and awareness across the organisation independent of levels, to ensure that risks are recognised. Many organisations have a dedicated risk management function or they seek external advice on a regular basis to ensure that risks are monitored and the organisations are in the know. Maintenance of a risk catalogue or risk register can be helpful in ensuring that a thorough review of all IT related risks takes place on a periodic basis and in providing assurance to the management that risks are being addressed.

Internal audit has an important role to play in assessing IT governance and it involves evaluating the adequacy and effectiveness of controls in responding to risks within the organization's governance, operations and information systems in connection with the following:

- Reliability and integrity of financial and operational information
- Effectiveness and efficiency of operations and programs
- Safeguarding of assets
- Compliance with laws, regulations, policies, procedures and contracts

The Audit Team should be conversant with the various aspects of the assignment. Internal audits of IT governance should focus on review of the following:

- The organization's implementation of governance practices clearly defined policies, roles, and responsibilities, tone at the top, management and clear accountability
- Consistency of government activities in assessing the degree to which such activities and standards are consistent
- Review of effective IT Governance practices - risk assessment, employee training, IT security etc.
- Compliance with the Audit Charter - conducting engagements as allowed by the audit charter and approved by the board
- Engagement with the IT Governance Body - ongoing discussion with the IT governance body to ensure that substantial organizational and risk changes are being addressed in a timely manner

Framework For Successful Implementation Of IT Governance

Globally recommended best practices have a three-pronged approach to address various organisational and process issues during the course of IT Governance implementation-

- Adopt an enterprise wide approach - business and IT should define the control requirements, IT should develop a customised control model applicable to all business units and a committee approach should be used for setting and implanting directions and policies

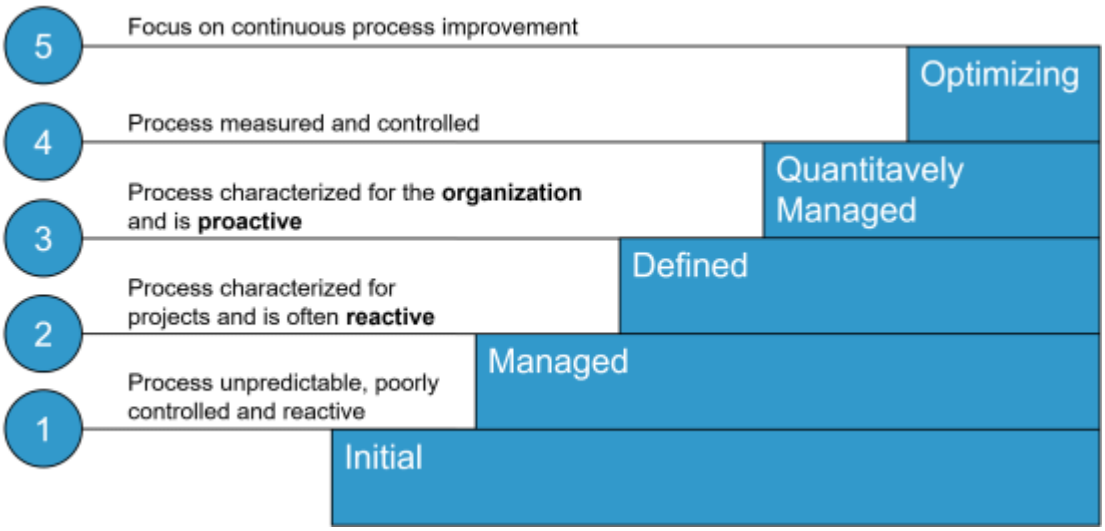
- Top level commitment and clear accountability – without the top management's mandate, IT Governance cannot succeed and it will fail should the there be no accountability between the business and the IT function

- An agreed IT Governance and control framework - stakeholder approval should be obtained to clarify the scope of IT Governance

The most notable governance frameworks are as under-

- Information Technology Infrastructure Library (ITIL) comprises five sets of best practices for service strategy, design, transition, operation and continual service improvement

- Capability Maturity Model Integration (CMMI) uses scale of 1 to 5 to gauge an organization's performance, quality and profitability maturity level as shown in the following diagram-



- Factor Analysis of Information Risk (FAIR) is relatively a new model that helps organizations quantify risk. It focusses on cyber security and operational risk for making more well-informed decisions

- Control Objectives for Information and Related Technology (COBIT) is a comprehensive framework of "globally accepted practices, analytical tools and models" for governance and management of enterprise IT. It is a structure of relationships and processes that controls the IT origination to achieve business objectives. It continues to be the most preferred IT Governance Framework

By following a formal framework, organizations can produce measurable results towards achieving their goals through IT Governance. Conceptually, IT Governance is still evolving. IT is a subset of the overall governance of an entity and its focus is on the management and control of information technology. It encompasses culture, organisation, policy and practices in the context of IT management and controls the following five key areas-

- Alignment – of IT and business with reference to services and projects
- Value Delivery – assess the Return on Investment by defining measurable KPIs
- Risk Management – assess IT risks and corresponding processes for risk mitigation
- Resource Management – facilitate oversight of IT funding at the enterprise level as well as to ensure adequacy of the IT capability and infrastructure
- Performance Measurement – measure the achievement of strategic IT objectives set by Directors

A Case Study In Context

With the integration of the IT Management System supported by the implementation of COBIT and the structuring of sustainability and process-based optimization model, Ecopetrol S.A., Columbia, has laid a strong foundation for the consolidation of IT governance, risk and compliance. Ecopetrol chose to implement 28 COBIT processes, giving priority to the control objectives that support Sarbanes-Oxley compliance. The Information Technology Division developed an internal exercise to determine the maturity level of these processes. After concluding that they were at an average maturity level of 2, the team identified the gaps and set up action plans to reach level 3 for the most critical processes

Background

Ecopetrol S.A. is Colombia´s largest integrated oil company with about 7,000 direct employees. It is among the top 40 oil companies in the world and the four largest oil companies in Latin America. In addition to Colombia, which accounts for 60 percent of Ecopetrol's total production, the company is involved in exploration and production activities in Brazil, Peru and the United States (Gulf of Mexico). Ecopetrol is also considerably increasing its participation in bio-fuels. The Forbes magazine annual list of the 2,000 largest companies in the world (April 2010) indicates that Ecopetrol is located at position 222, with the following information: Sales $14.26 billion, Profits $2.40 billion, Assets $27.20 billion and Market Value $54.14 billion.

The Corporate Governance Code of Ecopetrol comprises the best corporate practices needed to preserve the business ethics and the correct administration and control of the company. This enables the company to compete through recognition and respect for the rights of shareholders, investors and other stakeholders based on clear policies for transparency in the management and disclosure of information about the business, which will in turn generate greater confidence among stakeholders and the market in general. The internal control system of Ecopetrol is framed within international standards (COSO).

Process

The Information Technology Division chose COBIT as the proper IT governance framework to integrate an IT management system, based on the following characteristics of COBIT:

- Enables mapping of IT goals to business goals
- Results in better alignment based on business focus
- Provides a view of what IT does that is comprehendible by the management
- Indicates clear ownership and responsibilities based on process orientation
- Generally accepted by third parties and regulators
- Provides a shared understanding amongst all stakeholders based on a common language
- Fulfills the COSO and Sarbanes-Oxley requirements for the IT control environment

Ecopetrol's Information Technology Division defined the guidelines, processes and control objectives to implement. Similarly, the division identified the internal resources that would support the implementation of the system and allocated resources to hire the required external consultants.

The team established a project, giving special consideration to the following issues:

- Resource allocation and an interdisciplinary team with representatives from the involved areas within IT

- Defining the points of relationship with business units and other support units and interacting with key areas—finance, risk, strategy, quality and internal and external audit on an ongoing basis
- Integration and convergence with the IT support team in transport operations that was anticipating a COBIT implementation effort
- Alignment with business projects - strengthening of the internal control system (COSO) and compliance (Sarbanes-Oxley Act). We considered the various business initiatives and ongoing projects to ensure the coordination and integration of efforts
- A line of reporting at the highest level of management with weekly follow-up meetings on the project
- Identification of prior applications (Sarbanes-Oxley, high component in SAP) and other critical aspects for business process. Furthermore, understanding the people, resources and infrastructure associated with these applications

Ecopetrol chose to implement 28 COBIT processes, giving priority to the control objectives that support Sarbanes-Oxley compliance. The IT division developed an internal exercise to determine the maturity level of these processes. After concluding that it was at an average maturity level of 2, the team identified the gaps and set up action plans to reach level 3 for the most critical processes.

The project team then developed the design and documentation of the processes and subsequently facilitated the implementation and monitoring of the operations to complete the required adjustments. By June 2009, as a result, the Division had implemented and secured 14 high-priority COBIT processes and by December 2009, all 28 had been implemented.

In the following year, internal and external audits were developed for Sarbanes-Oxley compliance. Several measures were implemented for remediation and improvement of key IT processes and controls. As a result, the external auditor reported that there were no significant deficiencies or material weaknesses in IT controls that need to be reported by the CIO, the CFO, the CEO or the auditor.

At the end of this exercise, the COBIT project received a company award for excellence to recognize the project team's performance, initiative and teamwork.

Learnings

Key issues that led to the excellent results of the first year of COBIT implementation in Ecopetrol's IT management system include:

- The implementation of COBIT was structured as a project, with a detailed work-plan, with clearly defined milestones, a dedicated team with reliance on project management, risk management and control of timing and deliverables of the project
- The team had the management's support, providing weekly progress report and bringing up any deviations and actions that required assurance
- The company hired well-known consulting firms that integrated teams with extensive knowledge and experience
- The project was well integrated with all areas involved, leveraging synergies, especially with the IT support team in transport operations who provided the results of previous efforts and guaranteed the perspective of business users
- Maturity level assessments were conducted by a competent and independent third party
- More than 20 employees passed the COBIT Foundation exam and earned a COBIT certificate

(source: ISACA)

To Conclude

Developing a comprehensive IT governance program can be a daunting task even for organizations with mature management practices. A subject-matter expert's services can be a great enabler for implementing practical and proven strategies that formulate an IT governance program and road map. An expert can assist in engaging senior management and adopting organization-wide ITGC practices.

Prevailing organization and governance structures provide a good indication of whether IT supports the organization in achieving its strategic objectives. The tone at the top should support the culture of proactive IT Governance in an organization.

Strategic performance management is an integral component of an effective IT governance, enabling proper mechanisms to govern the needs of the organization and IT service delivery. Thus, the ultimate objective in IT Governance is to attain a higher level of maturity in a sustained manner to proactively mitigate the risks which may affect the business.

Use IT To Drive Performance

A maxim "Anything that is measured, is done" can be applied to IT Governance as well. In the absence of KPIs, IT Governance may remain an initiative which does not achieve its full potential. To attain a higher maturity level in IT Governance, performance measures should be based on targets derived from the IT function's objectives. Performance measurement systems should do the following-

- Focus on customers to increase customer satisfaction
- Improve processes so that problems are anticipated and prevented
- Identify the IT costs to reduce and optimise them
- Set realistic benchmarks for comparison

Performance can be measured as a mix of objective and subjective measures. A balance scorecard approach, if used, can cover financials, customer, internal and learning dimensions. These should be easy to comprehend and interpret and can be consolidated for hierarchical reporting. Ideally, KPIs that are limited in number and focused on measures should be prioritised to support decision making.

The following table indicates specific stakeholder objectives and corresponding performance measures which can improve IT governance-

Stakeholder	Objective	Requirements/ Areas of Interest
Investors	• Return on investments • Alignment of investment with strategic objectives	• Financial – RoI • Customer surveys and feedback • Capability benchmarks, performance exceptions • Learning – attrition, retention, skill profile, training and development
Controllers (auditors, risk and compliance officials, finance, HR, industry specific regulators)	• Monitoring risk and compliance • Evidence of governance and risk management • Compliance with strategy	• Financial – losses, investments in control improvements • Customer – exceptions/breaches, risk management, compliance with legislation • Processes - control effectiveness and compliance • Learning – risk identification and prevention
Providers (in-house and out-sourced consultants in IT delivery and support)	• Match customer expectations • Effectiveness and efficient service delivery • SLA compliance	• Financial – operations and project costs • Customer – SLA achievement and deviations • Processes - improvement in efficiency and risk reduction • Learning – capability to deliver, TAT for readiness of new ?, TAT for time to market