IT STRATEGY AND GOVERNANCE: FRAMEWORKS AND BEST PRACTICES

Vaishali Raodeo*

ABSTRACT

With IT at the core of most 21st century businesses, and with today's focus on compliance and risk management it is a necessity for every organization to think about IT governance. IT governance at its most basic is the process of making decisions about IT. By this simple definition, every organization has some form of IT governance. Good IT governance ensures that IT investments are optimized, aligned with business strategy, and deliver value within acceptable risk boundaries. Organizations assess their present and future IT requirements and develop a suitable framework to initiate IT governance activities at their place. However, several organizations fail to identify an appropriate IT governance framework matching their organizational needs.

Several models and frameworks are available today, developed on international standards, such as ITIL, COBIT, ISO, and Six Sigma. This paper discusses the main objectives of IT governance, examines the critical elements for effective IT governance and the need for incorporating it in the overall corporate governance framework. It also elaborates the best available and widely used industry standards in structuring IT governance framework.

Keywords: *COBIT, frameworks, Governance, IT compliance.*

*****Lecturer, Atharva Institute of Management Studies, Mumbai.

INTRODUCTION

In this digital era, Information Technology has become a core element for businesses. Organizations the world over are making large investments on acquiring IT capabilities to improve their operational efficiency and product quality, manage business risk and information security. IT has become instrumental in maximizing overall business value. As the dependence of organizations on IT has grown, their IT budgets have also grown substantially. Management of an IT firm optimizes IT investment and extract maximum value out of investment on IT resources. The strategic benefits and risks that these investments present, coupled with the new regulatory environment, necessitates board-level risk management and governance activities for IT.

IT governance enables the management to make better decisions pertaining to IT initiatives and investments. It basically provides a framework to fix responsibility center for the performance of IT in meeting the organizational goal, and justify the need for IT in terms of Return On Investments (ROI) and Economic Value Added (EVA). It provides several tools, guidelines and regulations- in fact, a comprehensive framework- to make decisions, monitor outcomes and take appropriate actions towards optimizing IT resources of an organization. IT governance also provides a clear structure of responsibility centers and corresponding decision authority within the IT domain, like any other functional domain of an organization.

Corporate governance is about promoting corporate fairness, transparency and accountability whereas IT governance is defined as the focus of IT decision-making authority. IT is a subset discipline of corporate governance and is focused on IT systems and their performance and risk management.

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 organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives.

ISACA created the ITGI to assist enterprise leaders in their responsibility to ensure that IT goals align with those of the business by ensuring that IT delivers value, performance is measured, resources are allocated properly, and risks are mitigated.

The growing need for IT governance tools and techniques was fueled by the following factors

- Growing complexity of IT environments
- Fragmented or poorly performing IT infrastructures
- Users frustration leading to ad hoc solutions

- IT costs perceived to be out of control
- IT managers operating like firefighters
- Communication gap between business and IT managers
- Increasing pressure to leverage technology in business strategies
- Need to comply with increasing laws, standards, and regulations
- Scarcity of skilled staff
- Lack of application ownership
- Resource conflicts
- Impaired organizational flexibility
- Concern for risk exposures
- Volatile organizational, political, or economic environment

IT GOVERNANCE MATURITY MODEL

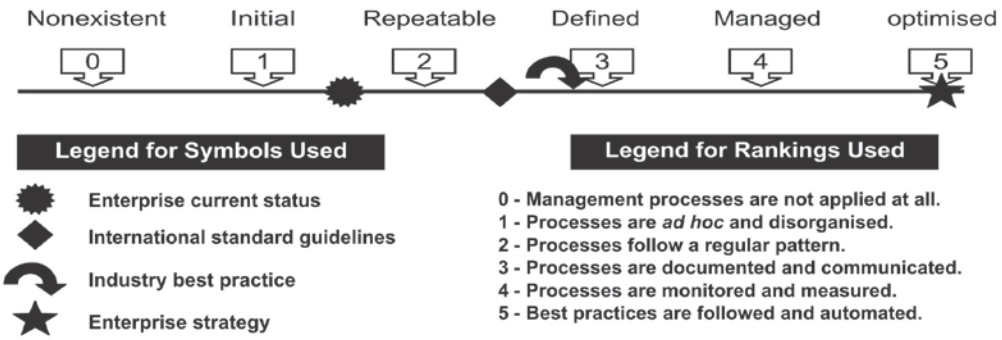

Fig 1 IT Governance Institute maturity scale

ITGI developed a maturity model for the internal control of IT that provides to organizations a pragmatic and structured approach to measuring how well developed their processes are against a consistent and easy-to-understand scale. The maturity model was fashioned after the one originated by the Software Engineering Institute (SEI) for software development.

ITGI expanded the basic concept of the maturity model by applying it to the management of IT processes and controls. The principles were used to define a set of levels that allow an organization to assess where it is relative to the control and governance over IT. These levels are presented on a scale that moves from nonexistent on the left to optimize on the right. By using such a scale, an organization can determine where it is and define where it wants to go, and if it identifies a gap, it can do an analysis to translate the findings into projects. Reference points can be added to the scale. Comparisons can be performed with what others are doing if those data are available, and the organization can determine where emerging international

standards and industry best practices are pointing for the effective management of security and control.

GEIT

As per 'Global Status Report on the Governance of Enterprise It '(Geit)—2011 , designed and created by ITGI, there are still significant opportunities for many enterprises to transition IT's role to a more pro-active one. This can be done through the use of mechanisms such as GEIT boards, an appropriate organization structure encompassing roles for managing business relationships, and standardized processes to effectively bridge the business demand with the IT supply. IT innovation offers ample opportunities for IT to play a more pro-active role.

The survey covered both large and small enterprises in 21 countries, 10 industries. The report revealed a significant degree of accord on the contribution of IT to business success, the challenges and opportunities connected with IT, the impact of the economic crisis. The report is based on response from 834 business executives and heads of information technology (IT) and their view about role of IT in their enterprise.

Key findings of the report are

- Value creation of IT investments is one of the most important dimensions of IT's contribution to the business. But challenges like increasing IT costs and an insufficient number of IT staff are the most common IT-related issues.
- Governance of enterprise IT (GEIT) is a priority with most enterprises. The main driver for activities related to GEIT is ensuring that IT functionality aligns with business needs, and the most commonly experienced outcomes are improvements in management of IT-related risk and communication and relationships between business and IT.
- Outsourcing is highly prevalent across the board, especially in larger enterprises and those where IT is considered important to the delivery of the business strategy or vision.
- Around 60% IT firms use or are planning to use cloud computing for non-mission-critical IT services, and more than 40% use or are planning to use it for mission-critical IT services. For companies that do not have plans to use cloud computing the main reasons are data privacy and security concerns.

- The global economic downturn has had an effect on IT activities, like reduction incontractor staff, reduction in permanent staff and a consolidation of the infrastructure.

Successfully implementing GEIT depends on several factors: change management, communication, proper scoping and identification of achievable objectives. And the outcomes of a successful implementation are worth it, producing both shorter-term, tangible benefits such as reduced cost and longer-term benefits such as enhanced management of IT-related risk, improved relationships between business and IT, and increased business competitiveness.

The use of frameworks and structures can help improve the governance of enterprise architecture. Frameworks and standards such as COBIT, ITIL, ISO 27000 series and TOGAF can help improve GEIT, bringing structure and clarity to areas such as service management, information security and enterprise architecture. COBIT provides an overarching framework within which the more focused frameworks and standards can be applied more effectively. Similarly, structures such as an architecture review board can improve the re-use of and synergies between initiatives ensure that total cost of ownership is considered, and help reduce complexity and increase agility over time.

STANDARDS AND FRAMEWORKS

According to the IT Governance Institute, IT governance "is an integral part of enterprise governance and consists of the leadership and organizational structures and processes that ensure that the organization's IT sustains and extends the organization's strategies and objectives."

Implementing good IT governance requires a framework based on three major elements:

- Structure: Organizational structure and responsibility of decision making
- Process: The decision-making processes for proposing investments, reviewing investments, approving investments
- Communication: The way of monitoring and measuring the results of these processes and decisions. Mechanisms to communicate IT investment decisions to the board of directors, executive management, business management, IT management, employees, and shareholders

Fig 2 IT Governance focus areas

EXISTING FRAMEWORKS

While there is no single, complete, off-the-shelf IT governance framework, there are a number of frameworks available that can serve as useful starting points for developing a governance model.

As a result, most IT organizations today are "rolling their own" models, but borrowing heavily from existing frameworks. Most of the existing frameworks are complementary, with strengths in different areas.

CAPABILITY MATURITY MODEL (CMM/CMMI)

The capability Maturity Model (CMM), developed by Software Engineering Institute (SEI) is a well accepted and widely used standard to ensure software quality. The CMM framework is essentially used in software services industry to measure and evaluate the various maturity levels of a software development process on a scale of 1 to 5. SEI released an advanced version of CMM known as the capability Maturity Model Integration (CMMI) which consists of guidelines that are practiced throughout various phases of product development and maintenance. CMM framework is often used as a reference model for organizations implementing IT governance. CMM provides guidance for improving an organizations processes and its capability to manage the products and services. CMM measures the processes at five levels of maturity- Initial, Repeatable, Defined, Managed and Optimizing.

Level 1 Initial: System development projects follow no prescribed process.

Level 2 Repeatable: Project management processes and practices are established to track project costs, schedules, and functionality.

Level 3 Defined: A standard system development process is purchased or developed. All projects use a version of this process to develop and maintain information systems and software.

Level 4 Managed: Measurable goals for quality and productivity are established.

Level 5 Optimizing: The standardized system development process is continuously monitored and improved based on measures and data analysis established in Level 4.

COBIT

Control Objectives for Information and related Technologies (COBIT) was developed by the Information Systems Audit and Control Association (ISACA) and is now issued and maintained by the IT Governance Institute (ITGI) as a framework for providing control mechanisms over the information technology domain. Now in its third edition, COBIT has been extended to serve as an IT governance framework by providing maturity models, critical success factors, key goal indicators, and key performance indicators for the management of IT.

At the heart of COBIT are 34 high-level control objectives. These control objectives are grouped into four main domains: planning and organization, acquisition and implementation, delivery and support, and monitoring. Corresponding to each of the 34 control objectives are 318 detailed control objectives. COBIT represents a comprehensive framework for implementing IT governance with a very strong auditing and controls perspective, which has increasing resonance in the era of Sarbanes-Oxley and other compliance-related regulations and legislation.

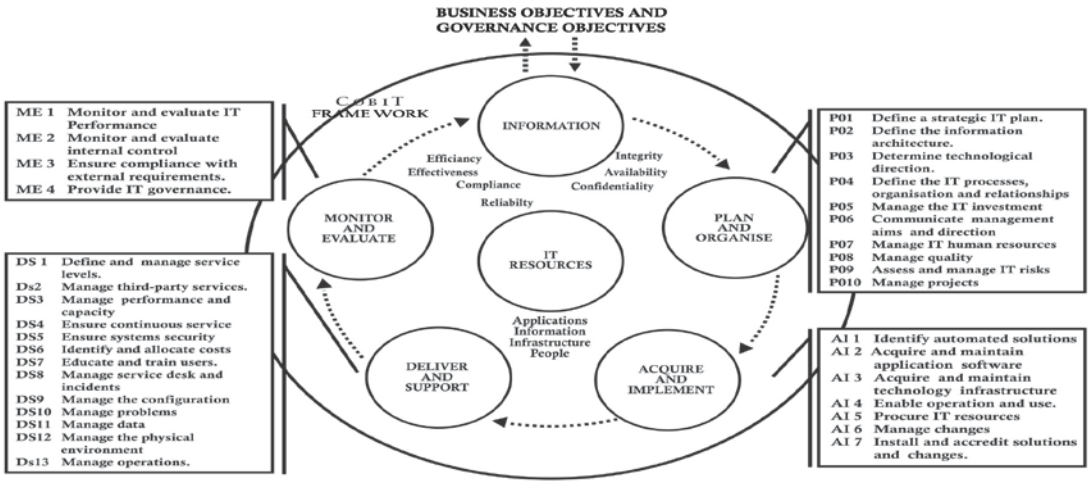

Fig 3 CoBIT framework

ITIL

The IT Infrastructure Library (ITIL), initially developed in the UK by the Office of Government Commerce (OGC), is gaining traction in the global IT community as a framework for IT governance. The library currently consists of eight books, including: "Software Asset Management," "Service Support," "Service Delivery," "Security Management," "Application Management," "ICT Infrastructure Management," "The Business Perspective," and "Planning to Implement Service Management". ITIL is focused on identifying best practices in regards to managing IT service levels and is particularly process-oriented.

While COBIT takes the perspective of audit and control, ITIL takes the perspective of service management. The two frameworks are more complementary than competitive and components of both can be taken to build a governance framework.

ISO 17799

The International Organization for Standardization has developed the third major governance framework, ISO 17799, titled "Information Technology — Code of Practice for Information Security Management." It was first released by the ISO however; it is based on British Standard 7799. The intent of the standard is to focus on security and aid an organization in the creation of an effective IT security plan.

The standard has the following high-level groupings: security policy, organizational security, asset classification and control, personnel security, physical and environmental security, communications and operations management, access control, systems development and maintenance, business continuity management, and compliance.

ISO 17799's relatively narrow focus on security makes it unsuitable as the sole basis for an IT governance framework, but since risk management is a component of IT governance, there is relevance to ISO 17799, and parts of it can be adopted in building an overall IT governance framework.

THE BENEFITS OF STANDARDS

There are a number of compelling reasons to adopt a defined standard:

1. Standards - Instead of spending time and effort to develop a framework based on limited experience, internationally developed existing standards can be taken as a base for governance activities.

2. Structured - The framework of the models provides an excellent structure that organizations can follow. The structure helps everyone to be on the same level because they can see what is expected.
3. Best Practices - The standards have been developed over time and assessed by hundreds of people and organizations all over the world. The cumulative years of experience reflected in the models can not be matched by a single organization's efforts.
4. Knowledge Sharing - By following standards, people can share ideas between organizations, profit from user groups, web sites, magazines, books and so on. Proponents of company-specific ad hoc approaches do not have this luxury.
5. Auditable - Without standards, it becomes far more difficult for auditors, especially third-party auditors, to effectively assess control. It means that the auditors themselves should be following standards, as opposed to ad hoc auditing practices. The goal must be to at least certify the organization against at least one base standard and then make recommendations over and above the standards, where appropriate.

COBIT is strong in IT controls and metrics. ISO 17799 covers IT security quite well and ITIL emphasizes processes, notably those surrounding the IT helpdesk.

IT GOVERNANCE SUCCESS FACTORS

- Effective decision-making and a strong focus on process

  Gartner Research former Vice President Michael Gerrard suggests that CIOs and IT managers start by defining the goal for each aspect of IT governance. The processes that support those objectives must address IT operational areas like security policy, business continuity policy, IT architecture, development standards, supplier policies, centralization vs. decentralization of IT management and resources, and ownership and usage policy and processes.

- IT project and systems portfolios that are aligned with business priorities

  Although project portfolio management should serve as an important process in an IT governance context, CIOs should understand that portfolio management processes also apply to the IT systems and non-project work the rest of the business depends on.

- Satisfied customers

  The success of IT governance depends on how IT managers and employees manage and fulfill customer requests. Even if this task is highly unpredictable, difficult to manage and guide without proper processes and documentation, it has to be managed

and measured if CIOs are to fully understand the cost of systems, projects and the overall effectiveness of operations.

- Strong decision-making by high-performing IT employees

  Effective IT governance includes the assignment of decision-making responsibility and if IT employees are to make decisions that support higher-level business objectives, their performance should be evaluated on the equality of their decision-making.

- An efficient, cost-effective IT department

  CIOs should demonstrate their departments' efficiency through up-to-date documentation and metrics. IT governance programs can also improve relations between IT and the business.

- Complete audit capabilities supporting each of these points

  Processes play an important role in effective IT governance, but those processes must be documented and continually monitored. Proper governance requires accountability as well as measurement. Processes and procedures must be detailed and documented, to show that IT has a consistent approach to solving the issues across the company. Governance is essential to ensure that an enterprise derives maximum value from its IT investments.

CONCLUSION

With the increasing significance of the role of IT and mounting IT budgets in today's organizations it is a common practice to introduce IT governance practices to establish a balance in value vs. cost of IT. The right governance enablers can ensure the transparency of IT supply and demand and facilitate decision making about demand and its prioritization in pursuit of value delivery to the enterprise.

REFERENCES

1. Craig Symons (Mar 29, 2005), " It Governance Framework"
2. "Creating an Effective IT Governance process," by Michael Gerrad;@ Gartner Inc: Nov.20, 2003
3. Chris Davis, Mike Schiller, Kevin Wheeler (2007), "IT Auditing using controls to protect information assets" Tata McGraw-Hill Publishing Company Ltd
4. Dr. Gad J. Selig, PMP, COP,"*Implementing IT Governance*: A Practical Guide to World Class IT Management Using Current & Emerging Best Practices" (2008)

5. George Spafford (April 22, 2003), "The Benefits of Standard IT Governance Frameworks — Datamation_com.htm
6. Hamakar,S,and Hutton,A, "Principles of IT Governance." Information Systems Control Journal, Volume2, 2004
7. IT Governance Institute(ITGI), COBIT, 4th Edition, December 2005. http://www.isaca.org
8. IT Governance Institute (2011), "Global Status Report on the Governance of Enterprise It (Geit)—2011"
9. Kenneth G Rau, " Effective Governance of IT: Design, Objectives, Roles and Relationships", Information System management Journal, Fall 2004.
10. Mary Beth Chrissis, Mike Konrad, Sandy Shrum, "Introduction to CMMI for development" a chapter of "Guidelines for Process Integration and Product Improvement", 3rd Edition.
11. http://www.informit.com/articles/article.aspx?p=1686446 MMI lopment: Guidelines for Process Integration and Chris Davis, Mike Schiller,
12. Ravi Kumar Jain B, (2006), "IT Governance An Introduction" ICFAI University press.
13. White paper, Callio Technologies, Jacqelin Bisson & Rene Sain-Germain, "The BS 7799/ISO 17799- For a better approach to information security".
14. www.infodom.hr/documents/White_Paper_ISO_17799_en.pdf
15. www.isaca.org
16. www.itil.co.uk