

# COBIT 4.1 – GOVERNANCE FRAMEWORK FOR EFFECTIVE ENTERPRISE IT

*R Vittal Raj*  
*FCA, CISA, CISSP, CISM, CIA, CFE*

**Abstract:** With IT now in the driver's seat, organisations globally have been struggling to make IT naturally responsive to business demands. While most IT managements are increasingly harbouring the dreams of a robust management framework for IT but often feel lost or frustrated. The session provides an overview of COBIT 4.1 and its components, and discusses how successful enterprises are using COBIT 4.1 from ITGI for effective IT Governance that supports and extends enterprise governance thereby enhancing enterprise value.

## 1. Is there a need to Govern IT?

For most organizations, IT, today, is a vital determinant of business performance and growth and for those organizations that do not realize this, improperly understood and mis- managed IT can be an inhibitor of business performance and growth, and may also prove fatal. Traditionally, IT has been relegated in its importance merely as one of the support functions. In reality, for any organization in any sphere of business, IT is responsible for processing, managing and delivering its life energy – Information. Information that supports effective decision making on seizing business opportunities, striking right strategies, operationalising day to day business processes, identifying and responding to business risks and in leading from the front.

IT Governance is the critical differentiator that separates organizations that have successfully leveraged on IT to lead their business and those that have not. Much different from mere IT management, IT governance starts at the helm of the enterprise, considers the larger picture and lays emphasis on relationships. As ITGI defines it:

“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”

- ITGI

Hence there is need for:

- Top management to recognize and lead through demonstrative leadership for IT Governance
- Ensuring IT direction is governed by business requirements by aligning IT strategy with the business strategy
- Providing a common language for IT, Top management, auditors and other stakeholders, to define expectations, thereby enabling enterprise wide synchronisation
- Putting in place organizational structures that will facilitate implementation of strategies and goals
- Ensuring that IT risks are managed
- Ensuring that investments in IT are delivering value and measuring performance
- Ensuring that IT resources are used responsibly

## 2. Challenges in managing Enterprise IT

IT Governance, to many, is a boring, clumsy, hazy, utopian, theoretical subject...good for a classroom session that is best forgotten once you are out of it...but can you really wish it away? Yes you certainly can, if information gets delivered to all your stakeholders, meets or still better exceeds their expectations. But reality is different – most organizations are saddled with problems with IT that seem to be eternally entangled. IT and users never seem to understand each other’s expectations and problems, IT feels that the top management does not give an ear to IT’s demands but seemingly supports business users who go about nailing IT for enterprise targets not met, on the other hand top management feels IT never becomes accountable for its performance and

ROI, mismanages IT risks that lead to business losses and so on. Most top managements and IT managements feel deadlocked over making IT deliver to business expectations.

The problem is to identify what & where exactly is the problem? Most managements are caught up with difficult questions:

- Why is IT not delivering to expectations, even though IT objectives are being set?
- How to make IT and its users see each others expectations?
- What are the IT resources that need to be managed and prioritized?
- How to drive process based IT and How to define controls for IT processes?
- How to assign roles and responsibilities for the various activities?
- How to establish measures that can be appreciated by both business and IT?

### **3. Overview of COBIT4.1 ® Framework**

COBIT or Control Objectives for Information and related technology was conceived by the IT Governance Institute as business-focused, process-oriented, controls-based and measurement-driven framework. COBIT has identified 34 IT processes that are categorized into FOUR domains.

#### *Business-focused*

IT from a business focus is recognized as the key differentiator of the COBIT Framework. COBIT looks at IT not for IT sake but for business sake and delivers to the multi-dimensional set of stakeholders primarily the Management, Users and Auditors. Thus the key business requirements of quality, security and fiduciary are addressed.

COBIT recognises the key theme that - To achieve business objectives, enterprises require information and this in turn requires investment in and management of IT resources that further need to be controlled through a set of structured processes such that IT delivers the information that will support and extend the business objectives.

Information criteria is a key component of COBIT that enables defining the control requirements through seven criteria viz. effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability.

IT Resources in COBIT are defined in four categories of Application, Information, Infrastructure and People.

#### *Process-oriented*

In order to achieve IT objectives, various activities and tasks need to get done and to ensure the right direction and consistency of such activities, these need to be organized into sub-processes which further are categorized into processes. COBIT groups the various activities into four broad domains :

- Plan and Organise (PO)– Provides the required direction for meeting the information delivery expectations of the stakeholders
- Acquire and Implement (AI) – Outlines what needs to be set up to enable service delivery as per expectations
- Deliver and Support (DS) – Deals with delivering services and solutions in a manner that meet user expectations
- Monitor and Evaluate (ME) – Monitors the various processes to ensure that the planned and expected services are being delivered and resolve deviations

Once the business objectives and the related information requirements have been understood, the investment in right IT resources need to be supported by clearly defined set of IT activities and processes that will deliver the desired information.

### *Controls-based*

COBIT is built on a strong controls foundation, which embrace on the Plan-Do-Check-Correct circle that delivers effective and consistent risk management. Control Objectives are defined for each of the 34 IT processes and designed to provide reasonable assurance that the business objectives will be achieved and undesired events will be prevented or detected and corrected. Control Objectives outline the high level requirements that management needs to get done to achieve control over the IT process. Detailed control objectives are defined for each of the 34 IT processes, that represent the key facets of control, if implemented would provide reasonable assurance on the achievement of the objectives.

Processes generally fail to deliver due to lack of ownership, lack of clear policies and procedures, improperly defined roles and responsibilities and inability to measure process performance. Further COBIT also identifies generic process control requirements that lay down the fundamental principles that need to be considered alongwith the detailed control objectives.

Amongst the reasons for poor controls are ambiguous understanding of what business benefits should be expected from IT processes and the underlying IT performance parameters, lack of clarity on assignment of roles and responsibilities, process inputs and outputs and metrics for measurement of outcomes and performance. COBIT provides an approach to resolving the above concerns. The RACI (Responsibility, Accountability, Consulted and Informed) Chart is an effective guide to assignment of roles and responsibilities for key IT activities in each process.

### *Measurement-driven*

One of the historic dilemma dogging managements is the question on how to measure IT performance. COBIT presents with tools to measure IT performance at various levels. Performance metrics in COBIT are linked right from the IT activity level to the super seceding IT process to the related IT goal and thereby the related business goal. COBIT makes it possible to identify the root cause of any business outcome to its IT goal that can further be traced to the underlying IT process(es) and thereby IT activities. For eg. a security breach leading to a reputation loss to the enterprise can be traced to the failure of the relevant IT goal of ensuring no attacks result in business impact, the underlying failure of the Access Control process to prevent unauthorized network access and the failure of access management and monitoring activities . Hence measures enable motivating and in also identifying root cause of failures at the IT strategic, tactical and operational level.

The COBIT Maturity Model is a valuable tool that enables measurement of IT process maturity and answer top management questions on “Where are we?” and “Where we want to be?”. The maturity model also enables inter and intra industry benchmarking. Without being rigid, the maturity model enables every organization to assess its current IT process maturity and assist in deciding its target state. Based on the maturity measurement, the organization can identify the control objectives and related activities that need to be improved. Further based on risk and value drivers, it also provides valuable guidance on, what controls the organisation needs to apply.

#### **4. COBIT 4.1 – Who can benefit from it ?**

COBIT addresses the interests of various stakeholders primary amongst which are:

- Executive Management
- Business Management and Users
- IT Management
- IT Assurance Professionals

<i>Whom</i>	<i>What questions can COBIT help answer?</i>
<i>Executive Management</i>	<p><i>Is IT delivering value and are IT risks being managed efficiently?</i></p> <p><i>Is the investment in IT delivering value while balancing risks</i></p> <p><i>How well are we managing our IT and where do we stand amongst our competitors?</i></p>
<i>Business Management &amp; Users</i>	<p><i>How to define business requirements from IT?</i></p> <p><i>How well are IT services being delivered in a controlled manner?</i></p> <p><i>How to derive assurance on the delivery of IT services?</i></p>
<i>IT Management</i>	<p><i>How to understand the business requirements and expectations from IT?</i></p> <p><i>What needs to be done to achieve the desired business outcomes from IT?</i></p> <p><i>How to measure the performance of IT processes and activities?</i></p>
<i>IT Assurance Professionals</i>	<p><i>How do we know IT processes are controlled?</i></p> <p><i>How do we substantiate our opinion on controls in IT?</i></p> <p><i>How do we advise on improvements in IT process that will lead to better achievement of objectives?</i></p>

COBIT provides a structured IT control framework that addresses the needs of various stakeholders that results in:

- Better alignment of IT to business needs
- Provides a common language for the IT users and the IT management
- Provides a process oriented, controls based framework for consistent delivery of value from IT while balancing risks
- Is widely recognized and acceptable since based on globally accepted frameworks of control and drawing from established regulatory principles, hence acceptable to multi-various stakeholder requirements.