Scoping Information Technology (IT) Enabled Services by Using COBIT 5

Enterprises today in the rapidly changing digital world are inundated with new demands, stringent regulations and risk scenarios emerging daily, making it critical to effectively govern and manage information and related technologies. This has resulted in enterprise leaders being under constant pressure to deliver value to enterprise stakeholders by achieving business objectives. This has made it imperative for management to ensure effective use of information and technology investments and related IT for not only supporting enterprise goals but also to maintain compliance with internally directed and externally imposed regulations. This dynamic changing environment provides a challenge for chartered accountants as assurance providers to provide assurance with the required level of confidence. However, with the right type of skills and toolsets this provides an excellent opportunity for chartered accountants to act as consultants who provide relevant IT enabled services. A key component of this knowledge base is usage of globally accepted good practices and frameworks and developing a holistic approach which meets the needs of stakeholders. This article provides an overview of how COBIT processes are structured and explains how to scope the assignment with example of recommended approach for selecting the relevant processes and good practices of COBIT. This can be used as a model for providing IT enabled services.

Using COBIT to Meeting Different Stakeholder Needs

For using COBIT, it is important to understand that COBIT 5 has been engineered to meet expectations of multiple stakeholders. It is designed to deliver benefits to both an enterprise's internal stakeholders, such as the board, management, employees, etc. as well as external stakeholders - customers, business partners, external auditors, shareholders, consultants, regulators, etc. It is written in a non-technical language and is therefore usable not only by IT professionals and consultants but also by senior management personnel, assurance providers, regulators for understanding and addressing IT-related issues as relevant to them. Globally from the GRC perspective, COBIT (www.isaca.org/cobit) has been widely used with COSO (www.coso.org) by management, IT professionals, regulators and auditors (internal/external for implementing or evaluating Governance and management practices from an end-to-end perspective. COBIT has been used an umbrella framework under which other standards and approaches, such as ITIL, ISO 27001, etc. have been integrated into overall enterprise governance. Diagram 1 provides sample examples of the different stakeholder needs which can be met by using COBIT 5.

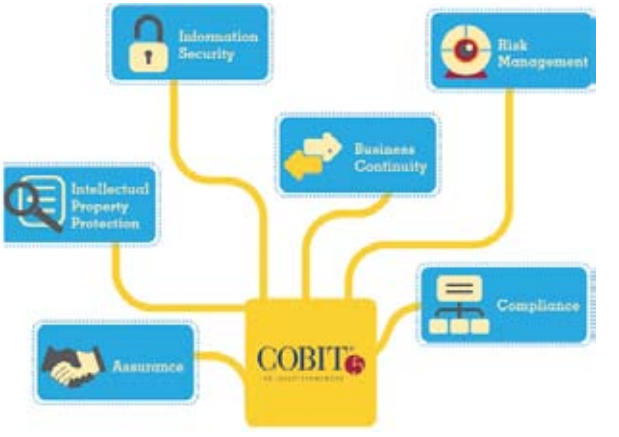

Diagram 1

Governance Domain and Processes

The COBIT 5: Enabling Processes guide publication provides a brief introduction to the COBIT concepts and provides the comprehensive contents covering the "process" enabler. COBIT 5 covers all functions and processes within the enterprise. It does not focus only on the IT function, but treats information and related technologies as assets that need to be dealt with the same way as any other asset by everyone in the enterprise. It is organised into five domains with clear demarcation between Governance and Management processes and practices. The Governance processes deal with the stakeholder governance objectives: value delivery, risk optimisation and resource optimisation and include practices and activities aimed at evaluating strategic options, providing direction to IT and monitoring the outcome (Evaluate, direct

CA A. Rafeq, The author is a fellow member of ICAI and can be reached at rafeq@vsnl.com.

and monitor [EDM] in line with the ISO/IEC 38500 standard concepts). The Governance domain contains five governance processes; within each process, evaluate, direct and monitor (EDM) practices are defined. These are:

1. Ensure governance framework setting and maintenance.
2. Ensure benefits delivery.
3. Ensure risk optimisation.
4. Ensure resource optimisation.
5. Ensure stakeholder transparency.

Management Domain and Processes

The management domain is based on the principles of PBRM (Plan, Run, Build and Monitor) as shown in Diagram 2. It and has totally 32 processes and covers enterprise activities end-to-end (i.e., all business and IT function areas), making the involvement, responsibilities and accountabilities of business stakeholders in the use of IT more transparent.

Diagram 2

Understanding Structure of COBIT 5 Enabling Process Knowledge Base

COBIT 5 provides complete, consistent, and easily navigable guidance to help promote access of information and assist in meeting any applicable legal, regulatory and contractual requirements. The good practices for each of the 37 processes (5 relating to governance and 32 relating to management) are presented consistently in a generic structure which makes understanding and using them easier. Understanding the structure of one process is sufficient as the same structure is consistently used for all processes. The generic structure of the process is explained below:

- Process identifier
  - Process label: The domain prefix (EDM, APO, BAI, DSS, MEA) and the process number
  - Process name: A short description, indicating the main subject of the process. (Example: EDM 03 Ensure Risk Optimisation)
- Area of the process: (Example: Governance or management)
- Domain name: (For example: Evaluate, Direct and Monitor)
- Process description: An overview of what the process does and a high-level overview of how the process accomplishes its purpose.
- Process purpose statement: A description of the overall purpose of the process.
- Goals cascade information: Reference and description of the IT-related goals that are primarily supported by the process and related metrics to measure the achievement of the IT-related goals.
- Process goals and metrics: A set of process goals and a limited number of example metrics.
- RACI chart: A suggested assignment of level of responsibility for process practices to different roles and structures. The enterprise roles listed are shaded darker than the IT roles. The different levels of involvement are:
  - R(esponsible): Who is getting the task done?
  - A(ccountable): Who accounts for the success of the task?
  - C(onsulted): Who is providing input?
  - I(nformed): Who is receiving information?
- Detailed description of the process practices for each practice:
  - Practice title and description. Example: EDM1.01 Evaluate the governance system.
  - Practice inputs and outputs, with indication of origin and destination.
  - Process activities, further detailing the practices.
- Related guidance—References to other standards and direction to additional guidance

How to Scope IT Enabled Services Using Relevant Content from COBIT 5

The good practices of COBIT 5 can be used as relevant depending on stakeholder needs or scope and objectives of assurance/consulting assignment. The first step to using COBIT 5 is selecting the relevant processes based on needs/scope/objective. There are multiple approaches to navigate and select relevant processes and customising COBIT for use. The recommended approach which is based on extensive research by ISACA is given below:

1. Using the COBIT 5 Goals Cascade. This approach explained in detail in the COBIT 5 framework has the following steps:
   a. Identify Stakeholder needs and based on this select relevant Governance objectives from: Benefits Realisation, Risk optimisation and Resource optimisation. (Please refer Figure 3 of COBIT 5 Business Framework)
   b. Based on the Governance objectives, select the relevant enterprise goals from the list of 17 enterprise goals. (Please refer Figure 5 of COBIT 5 Business Framework)
   c. Based on the selected Enterprises Goals, select relevant IT-related Goals from the list of 17 IT-related goals. (Please refer Figure 22 of COBIT 5 Business Framework)
   d. Based on the selected IT-related goals, use the criteria of P (Primary) or S (Secondary) to select relevant COBIT 5 process. (Please refer Figure 23 of

COBIT 5 Business Framework)

e. Review the contents of this list and further filter the list based on relevance.
f. Use the relevant contents (Process description, purpose, Goals cascade and metrics, Process Goals and related Metrics, RACI Chart, practices with Input-output document references, list of activities and related guidance) to prepare the benchmark of COBIT as applicable to you.
g. Customise these extracted contents of COBIT 5 as relevant to your requirements by integrating with other frameworks and internal practices and integrate them with policies, procedures and practices and guidelines of the enterprise.

It is noted that the above approach has to be used with caution and the identified processes from this approach need to be validated and filtered based on relevance. Users may not have all the information to follow each of the steps. Then, they may skip earlier steps and directly start from enterprise goals mapping or IT related goals mapping and select the relevant IT processes.

Developing Customised Approach for Scoping Assignments

In addition to the approach given above, there are other approaches also which can be developed by users based on their experience and expertise of using COBIT. For example, a good understanding of the COBIT 5 Concepts and COBIT 5 Enabling process documents will enable a user to select relevant processes by a quick walk-through and reading of the COBIT 5 process description and purpose statements. Further, processes can also be selected by searching on key words as relevant to the needs. However, whatever approach is used, it is important to validate and customise the contents based on relevance.

The complete lists of 37 processes of COBIT 5 are given below. By reading the contents of each of the process, one can get good idea of what is covered in each of these processes. The contents from each of these processes or a combination of selected processes as relevant can be made for preparing the proposal which becomes starting point from discussion regarding scope and objective of the assurance/consulting assignment. Once the scope is agreed upon, the extracted contents from these processes can be customised and used as a benchmark for providing the required services.

Governance Domain Processes:

(EDM: Evaluate, Direct and Monitor)

EDM1 Set and Maintain the Governance Framework
EDM2 Ensure Value Optimisation
EDM3 Ensure Risk Optimisation
EDM4 Ensure Resource Optimisation
EDM5 Ensure Stakeholder Transparency

Management Domain Processes:

(APO: Acquire, Plan and Organise)

APO1 Define the Management Framework for IT
APO2 Define Strategy
APO3 Manage Enterprise Architecture
APO4 Manage Innovation
APO5 Manage Portfolio
APO6 Manage Budget & Cost
APO7 Manage Human Resources
APO8 Manage Relationships
APO9 Manage Service Agreements
APO10 Manage Suppliers
APO11 Manage Quality
APO12 Manage Risk
APO13 Manage Security

(BAI: Build, Acquire and Implement)

BAI1 Manage Programmes and Projects
BAI2 Define Requirements
BAI3 Identify & Build Solutions
BAI4 Manage Availability and Capacity
BAI5 Enable Organisational Change
BAI6 Manage Changes
BAI7 Accept & Transition of Change
BAI8 Knowledge Management
BAI9 Manage Assets
BAI10 Manage Configuration

(DSS: Deliver, Service and Support)

DSS1 Manage Operations
DSS2 Manage Service Requests and Incidents
DSS3 Manage Problems
DSS4 Manage Continuity
DSS5 Manage Security Administration
DSS6 Manage Business Process Controls

(MEA: Monitor, Evaluate and Assess)

MEA1 Monitor and Evaluate Performance and Conformance
MEA2 Monitor System of Internal Control
MEA3 Monitor and Evaluate Compliance with External Requirements

Conclusion

The key differentiator of COBIT 5 is that it can be customised for enterprises of all sizes, industries and geographies regardless of the technology platform or the enterprise architecture. A reading of the COBIT 5 framework publication (available as a free download) will provide understanding of the five key principles, seven critical enablers, overall architecture and process structure of COBIT. The key to successful use of COBIT, in addition to concept understanding is learning the practical approach of navigating and selecting relevant processes and related contents, integrating them with other frameworks and customising it as per needs of the assignment whether it is in assurance or consulting. COBIT 5 has a rich repository of knowledge which can be readily customised for building a suite of specific IT enabled services. The harmonious blend of five principles and the seven key enablers with excellent collection of good practices combined with the fact that COBIT 5 is hugely popular globally accepted framework makes it the most suitable framework for providing IT enabled services for chartered accountants and IT consultants. Research has confirmed that those who invest time in understanding and using COBIT 5 will definitely reap rich rewards and add value.

The COBIT 5 framework is available to all as a free download from ISACA at www.isaca.org/cobit. All figures/diagrams are adapted from publications of ISACA. ■