Using COBIT 5 – The Business Framework for the Governance and Management of Enterprise IT[1]

Enterprise governance is not only a management requirement but is also mandated by law. Information technology is key enabler of enterprises and forms the edifice on which the information and information systems are built. Implementing internal controls is not only a management requirement but is now a regulatory requirement as well. In India, Clause 49 listing requirements seek inter alia certification of governance, risks and control by auditors. In an IT environment embedding the right level of controls within the information systems, which provides information to users securely and safely and as per business requirements, is critical not only for ensuring business success but is also a key requirement for the very survival of the enterprise. In implementing internal controls in an IT environment, the legacy approach of considering Information Technology and its contents as boxes to be secured by the IT department is fraught with extreme risk. Both from regulatory as well as enterprise perspective, senior management need to be involved in providing direction on how governance, risk and control are implemented using a holistic perspective based on the need for harnessing the power of information and information technology from a business perspective. The annual survey of 2012 by AICPA on the top technology issues impacting CPAs and enterprises highlights the importance of implementing the right level of security and giving adequate importance to this key area. As per COBIT5 released by ISACA recently, Information is the currency of the 21st century enterprise. Information, and the technology that supports it, can drive success, but, it also raises challenging governance and management issues. This article explains the need for using the approach and latest thinking provided by globally recognised framework COBIT5 as a benchmark for reviewing and implementing governance and management of enterprise IT. It explains the principles and enablers of COBIT 5 and how it can be as an effective tool to help enterprises simplify complex issues, deliver trust and value, manage risk, reduce potential public embarrassment, protect intellectual property and maximise opportunities.

AICPA Survey of Top Technology Issues Impacting Enterprises and Practising CPAs

The American Institute of Certified Public Accountants (AICPA) conducts annual survey of top 10 technology issues impacting the profession and enterprises. The 2012 Top Technology initiatives from a public accounting perspective found that securing the IT environment is this year's top business technology priority for AICPA members. The survey revealed that advances in information technology have empowered CPAs to access and manage information just about anywhere, anytime. While CPAs value the benefits that technology has made possible - such as greater flexibility, efficiency and productivity in the use of information - they also are concerned with the increase in risks to information security. CPAs are increasingly being asked to solve information technology problems for current clients and prospective clients. The results of this survey are expected to provide valuable feedback regarding the technology concerns, which are of greatest importance over the next 12-18 months for CPAs in practice. The findings of the survey are equally applicable to Indian enterprises as the core IT issues are relevant for the Indian scenario also and hence the technology priorities are applicable to practising CAs in India.

2012 Top Technology Priorities, GEIT and COBIT 5

The top technology priorities as per AICIPA survey are given below:

1. Securing the IT environment
2. Managing and retaining data
3. Managing risk and compliance
4. Ensuring privacy
5. Leveraging emerging technologies
6. Managing system implementation
7. Enabling decision support and managing performance
8. Governing and managing IT investment/spending
9. Preventing and responding to fraud
10. Managing vendors and service providers

[1] CA A. Rafeq: The author, is a fellow member of the Institute. He can reached at rafeq@vsnl.com.

It may be seen that governance, risk and compliance (GRC) are at the core of all the above key technology priorities identified in the survey. Implementing effective GRC requires implementing Governance of Enterprise IT as an integral part of enterprise governance so that it meets not only compliance requirements but also adds value to the enterprise by balancing risk and return. Using a comprehensive framework such as COBIT 5 enables enterprises to achieve their objectives for the governance and management of enterprise IT. The best practices of COBIT 5 help enterprises to create optimal value from IT by maintaining a balance between realising benefits and optimising risk levels and resource use. Further, COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking in the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders. The key advantage in using a generic framework such as COBIT 5 is that it is useful for enterprises of all sizes, whether commercial, not-for-profit or in the public sector. Currently, the COBIT 5 product family includes the following products ready for use:

- COBIT 5 (framework): available as free download at www.isaca.org/cobit
- COBIT 5: Enabling Processes: free for members of ISACA.
- COBIT 5 Implementation guide: free for members of ISACA.

Need for Implementing Enterprise Governance and Governance of Enterprise IT (GEIT)

As per COBIT 5 implementation guide, GEIT is not an isolated discipline but an integral part of enterprise governance. While the need for governance at an enterprise level is driven primarily by delivery of stakeholder value and demand for transparency and effective management of enterprise risks, the significant opportunities, costs, and risks associated with IT call for a dedicated, yet integrated, focus on GEIT. GEIT enables the enterprise to take full advantage of IT, maximising benefits, capitalising on opportunities and gaining competitive advantage. GEIT is applicable globally for all type of enterprises—whether public or private, large or small as criticality of information is a key resource and the fact that IT is a strategic asset and important contributor to success is being increasingly being recognised. This makes it imperative for most enterprises to recognise information and ensure the use of IT as critical assets which needs to be governed properly. Further, the improvement of the governance of enterprise IT (GEIT) is widely recognised by top management as an essential part of enterprise governance. At a time when the significance of information and the pervasiveness of information technology are increasingly part of every aspect of business and public life, the need to drive more value from IT investments and manage an increasing array of IT-related risks has never been greater. Increasing regulation is also driving heightened awareness among boards of directors regarding the importance of a well-controlled IT environment and the need to comply with legal, regulatory and contractual obligations.

Need for Enterprises to Use COBIT 5

Enterprises depend on good, reliable, repeatable data, on which they can base good business decisions. COBIT 5 provides good practices in governance and management to address these critical business issues. COBIT 5 is a set of globally accepted principles, practices, analytical tools and models that can be customised for enterprises of all sizes, industries and geographies. It helps enterprises create optimal value from their information and technology. COBIT 5 provides the tools necessary to understand, utilise, implement and direct important IT-related activities, and make more informed decisions through simplified navigation and use. COBIT 5 is intended for enterprises of all types and sizes, including non-profit and public sector and is designed to deliver business benefits to enterprises, including:

- Increased value creation from use of IT; user satisfaction with IT engagement and services; reduced IT-related risks and compliance with laws, regulations and contractual requirements
- The development of more business-focused IT solutions and services
- Increased enterprise wide involvement in IT-related activities

Integrating COBIT 5 With Other Frameworks

COBIT 5 is based on an enterprise view and is aligned with enterprise governance best practices enabling GEIT to be implemented as an integral part of wider enterprise governance. COBIT5 also provides a basis to integrate effectively other frameworks, standards and practices used such as such as ITIL, TOGAF and ISO 27000. It is also aligned with The GEIT standard ISO/IEC 38500:2008 which sets out high-level principles for the governance of IT, covering responsibility, strategy, acquisition, performance, compliance and human behaviour that the governing body (e.g., board) should evaluate, direct and monitor. Thus COBIT 5 acts as the single overarching framework which serves as a consistent and integrated source of guidance in a non-technical, technology-agnostic common language. The framework and resulting enablers should be aligned with and in harmony with (amongst others) the:

- Enterprise policies, strategies, governance and business plans, and audit approaches
- Enterprise risk management framework
- Existing enterprise governance organisation, structures and processes

Customising COBIT As Per Need

COBIT 5 can be tailored to meet an enterprise's specific business model, technology environment, industry, location and corporate culture. Because of its open design, it can be applied to meet needs related to:

- Information security
- Risk management
- Governance and management of enterprise IT
- Assurance activities
- Legislative and regulatory compliance
- Financial processing or CSR reporting

Five Principles and Seven Enablers of COBIT 5

COBIT 5 simplifies governance challenges with just five principles and seven enablers. The five key principles for governance and management of enterprise IT in COBIT 5 taken together enable the enterprise to build an effective governance and management framework that optimises information and technology investment and use for the benefit of stakeholders.

Principle 1: Meeting Stakeholder Needs

Enterprises exist to create value for their stakeholders by maintaining a balance between the realisation of benefits and the optimisation of risk and use of resources. COBIT 5 provides all of the required processes and other enablers to support business value creation through the use of IT. Because every enterprise has different objectives, an enterprise can customise COBIT 5 to suit its own context through the goals cascade, translating high-level enterprise goals into manageable, specific, IT-related goals and mapping these to specific processes and practices.

COBIT 5 Goals Cascade

Every enterprise operates in a different context; this context is determined by external factors (the market, the industry, geopolitics, etc.) and internal factors (the culture, organisation, risk appetite, etc.), and requires a customised governance and management system. Stakeholder needs have to be transformed into an enterprise's actionable strategy. The COBIT 5 goals cascade is the mechanism to translate stakeholder needs into specific, actionable and customised enterprise goals, IT-related goals and enabler goals. This translation allows setting specific goals at every level and in every area of the enterprise in support of the overall goals and stakeholder requirements, and thus effectively supports alignment between enterprise needs and IT solutions and services.

Principle 2: Covering the Enterprise End-to-End

COBIT 5 integrates governance of enterprise IT into enterprise governance. It covers all functions and processes within the enterprise; COBIT 5 does not focus only on the 'IT function', but treats information and related technologies as assets that need to be dealt with just like any other asset by everyone in the enterprise. It considers all IT-related governance and management enablers to be enterprise-wide and end-to-end, i.e., inclusive of everything and everyone—internal and external—that is relevant to governance and management of enterprise information and related IT. The end-to-end governance approach that is the foundation of COBIT 5 is depicted below showing the key components of a governance system.

Principle 3: Applying a Single Integrated Framework

There are many IT-related standards and best practices, each providing guidance on a subset of IT activities. COBIT 5 is a single and integrated framework as it aligns with other latest relevant standards and frameworks, and thus, allows the enterprise to use COBIT 5 as the overarching governance and management framework integrator. It is complete in enterprise coverage, providing a basis to integrate effectively other frameworks, standards and practices used.

Principle 4: Enabling a Holistic Approach

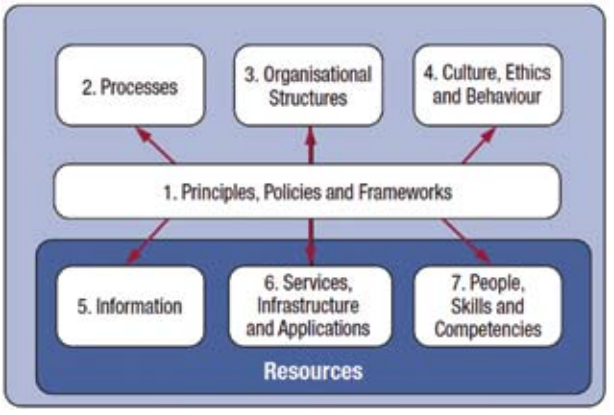
Efficient and effective governance and management of enterprise IT require a holistic approach, taking into account several interacting components. COBIT 5 defines a set of enablers to support the implementation of a comprehensive governance and management system for enterprise IT. Enablers are broadly defined as anything that can help achieve the objectives of the enterprise.

COBIT 5 Enablers

Enablers are factors that, individually and collectively, influence whether something will work— in this case, governance and management over enterprise IT. Enablers are driven by the goals cascade, i.e., higher-level IT-related goals define what the different enablers should achieve. The COBIT 5 framework describes seven categories of enablers:

1. Principles, policies and frameworks are the vehicle to translate the desired behaviour into practical guidance for day-to-day management.
2. Processes describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals.
3. Organisational structures are the key decision-making entities in an enterprise.
4. Culture, ethics and behaviour of individuals and of the enterprise are very often underestimated as a success factor in governance and management activities.

5. Information is pervasive throughout any organisation and includes all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed, but at the operational level, information is very often the key product of the enterprise itself.
6. Services, infrastructure and applications include the infrastructure, technology and applications that provide the enterprise with information technology processing and services.
7. People, skills and competencies are linked to people and are required for successful completion of all activities and for making correct decisions and taking corrective actions.



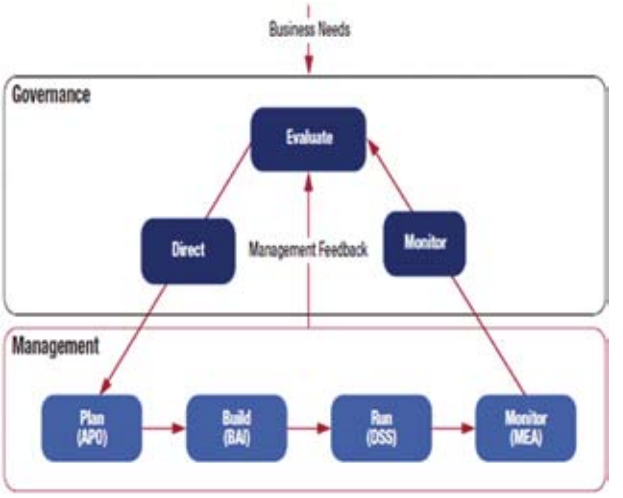
Principle 5: Separating Governance From Management

The COBIT 5 framework makes a clear distinction between governance and management. These two disciplines encompass different types of activities, require different organisational structures and serve different purposes.

Governance: ensures that stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives to be achieved; setting direction through prioritisation and decision making; and monitoring performance and compliance against agreed-on direction and objectives. In most enterprises, overall governance is the responsibility of the board of directors under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organisational structures at an appropriate level, particularly in larger, complex enterprises.

Management: plans, builds, runs and monitors activities in alignment with the direction set by the governance body to achieve the enterprise objectives. In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer.

From the definitions of governance and management, it is clear that they comprise different types of activities, with different responsibilities; however, given the role of governance—to evaluate, direct and monitor—a set of interactions is required between governance and management to result in an efficient and effective governance system.



COBIT 5 Process Reference Model

COBIT 5 includes a process reference model, which defines and describes in detail a number of governance and management processes. It represents all of the processes normally found in an enterprise relating to IT activities, providing a common reference model understandable to operational IT and business managers. The proposed process model is a complete, comprehensive model, but it is not the only possible process model. Each enterprise must define its own process set, taking into account its specific situation. Incorporating an operational model and a common language for all parts of the enterprise involved in IT activities is one of the most important and critical steps towards good governance. It also provides a framework for measuring and monitoring IT performance, providing IT assurance, communicating with service providers, and integrating best management practices.

Conclusion

This article is extracted from the contents of COBIT 5 framework released on 10th April 2012 and adapted from the perspective of CA. The objective of this article was to provide a brief overview of COBIT 5 and highlight the need for using globally accepted framework such as COBIT 5 for implementing GEIT which is the need of the hour. CAs have recognised that there is no escape from the domain of Information Technology as it increasingly impacts how electronic information and related controls are reviewed and accessed for providing compliance, assurance or consulting service for clients. Hence, it is imperative for CAs to update methodologies of how we provide services, ensure that the right tools are used to ensure quality of services to clients. IT is an area which is a constant state of continuous improvement. Hence, it is vital for CAs to keep on updating knowledge and skills sets and explore innovative ways of delivering services using IT and related best practices. Using globally recognised frameworks such as COBIT 5 enables CAs to provide value addition and also results in building brand image of being user of an approach and tool set based on the latest thinking and research. ■

Note: COBIT framework is available as free download from www.isaca.org/cobit. All figures used are courtesy of ISACA.