6 Tips for Implementing IT Governance With COBIT 5

By Juan Carlos Morales, CISA, CISM, CGEIT, CRISC

IT has become a strategic element to create opportunities, innovation and competitive advantage. However, it entails inherent risk related to confidentiality, integrity and availability of information that requires attention.

Delivering value to stakeholders requires good governance and management of IT (GEIT). COBIT® 5 provides a comprehensive framework that helps organizations to achieve their goals and create value through effective GEIT. The following are several tips for implementing IT governance or continuous process improvement using the COBIT 5 framework:

1. Obtain senior management support. A key success factor for COBIT 5 is top management providing the direction, mandate and ongoing commitment for the initiative, and all parties supporting the governance and management processes should understand the business and IT objectives. IT governance principle 1 (in chapter five of the King III report) states that the board is accountable for IT governance, should understand the strategic importance of IT, takes responsibility for IT governance and includes it on the organization’s agenda. King III further states, “International guidelines have been developed through organisations such as ITGI and ISACA (COBIT® and Val IT), the International Organization for Standardization (ISO) authorities (e.g., ISO 38500) and various other organisations such as OCEG. These may be used as a framework or audit for the adequacy of the company’s information governance for instance, but it is not possible to have ‘one size fits all’.”

2. Understand the external and internal organizational context and identify the relevant factors that may affect the ability to achieve business objectives. Whether one is engaged in an audit or implementing IT governance, a management system or a continuous improvement initiative, before starting, one needs to understand the organizational context and stakeholders’ needs. Principle 6 of the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework states that the organization must specify objectives with sufficient clarity to enable the identification and assessment of risk. The COBIT 5 framework focuses on business objectives using the goals cascade model and balanced scorecard (BSC) domains.

3. Identify pain points. Pain point identification creates the desire for change at the management level as the starting point for IT governance initiatives. It contributes to recognizing and accepting the need to implement an improvement initiative and create the required sense of urgency. Sometimes IT issues are only symptoms of a larger problem: poor or nonexistent IT governance.

4. Justify the project with a business case. A practical solutions implementation defines projects justified by business cases. A business case identifies the project benefits and enables compliance monitoring. The business case is a valuable business management tool to focus on value creation. A business case should include: business benefits, business changes needed, investment required, constraints and dependencies, roles, responsibilities and accountability, and a plan to monitor/measure benefit realization.

5. Focus on quick wins and prioritize the most beneficial improvements that are easiest to implement. Quick wins help to build credibility. Among the various improvement options, prioritize those that are most beneficial while also considering that it is necessary to give short-term results; therefore, select the easiest to implement. Principle 11 of the COSO framework indicates that the organization must select and develop general controls on IT. Control activities are part of the activities of the 37 COBIT 5 processes. Specifically, DSS06 Manage business process controls ensures that the control activities incorporated into business processes’ automated controls or application controls are properly managed.

6. Adopt and adapt the COBIT 5 framework to the unique context of the organization. Adopt and adapt best practices to meet the business approach to changes in policies and processes. COBIT 5 process guidance includes how the IT-related enterprise process practices and activities support the IT-related goals of “Managed IT-related business
risk,” “IT compliance and support for business compliance with external laws and regulations,” and “IT compliance with internal policies.” Principle 10 of the COSO framework indicates that the organization must select and develop control activities that contribute to the mitigation of risk to the achievement of objectives to acceptable levels. The COBIT 5 processes enabler guidance for the 37 COBIT 5 processes supports enterprises in their selection and development of control activities and other arrangements (e.g., structural segregation of duties), particularly with the practices and activities to consider for IT-related enterprise processes.

Juan Carlos Morales, CISA, CISM, CGEIT, CRISC
Is an IT governance and risk management consultant and trainer and COBIT 5 instructor accredited by APMG.

Endnotes

1 ISACA, COBIT 5 Implementation, USA, 2012, chapter 3
2 King Committee on Corporate Governance, The King Report on Corporate Governance (King III), South Africa, 2009
3 ISACA, COBIT 5 Implementation, USA, 2012, chapter 3 and chapter 6
4 The Committee of Sponsoring Organizations of the Treadway Commission (COSO), Internal Control—Integrated Framework, 2013
5 ISACA, COBIT 5 Implementation, USA, 2012, chapter 3
6 ISACA, COBIT 5 Implementation, USA, 2012, chapter 6 and Appendix D
7 ISACA, COBIT 5 Implementation, USA, 2012, chapter 3
8 ISACA, COBIT 5 Implementation, USA, 2012, chapter 3
9 ISACA, COBIT 5: Enabling Processes, USA, 2012

©2014 ISACA. All rights reserved.