Mapping COBIT 5 with IT Governance, Risk and Compliance at Ecopetrol S.A.

By Alberto León Lozano, CISA, CGEIT, CIA, CRMA

As part of an updated strategy, Ecopetrol S.A., a vertically integrated energy company, began a corporate transformation with the goals of growth and strengthening its internal control system. It knew it needed a clear approach for governance and management of IT services as well as best global reference standards and a framework, so it used the Committee of Sponsoring Organizations of the Treadway Commission (COSO) and COBIT frameworks, which helped consolidate strong IT governance practices that were totally aligned with the corporate internal control initiatives.

In 2007, Ecopetrol updated its corporate strategy, which required important changes and improvements in the organizational structure and processes that support the strategic objectives. Consequently, important milestones, such as the transformation of the legal nature of the company, the initiation of international operations and the adoption of the COSO Internal Control—Integrated Framework, were put in place to strengthen the internal control system. The company listed its shares on the New York Stock Exchange (NYSE) beginning in September 2008.

Aligned with the strategic deployment and to provide timely and effective responses to the requirements generated by the company’s situation, Ecopetrol’s Information Technology Division (DTI) decided in 2008 to integrate an IT management system, based on a proper framework. COBIT® was selected as the appropriate IT governance framework to implement its IT management system.

The IT management system incorporated the COBIT® 4.1 framework to cover the key IT control objectives that support the reliability and security of the company’s information. During the last five years of the IT management system operation, IT risk management and compliance have been successful. However, DTI has remained on constant alert to the challenges of growth and operational excellence that the company established. The objective is to incorporate the best practices that promote the sustainability of these results.

Following the release of COBIT® 5, DTI established a strategy to extend the current practices, ensuring the alignment and stability of the system, by expanding to new management and governance practices.

This article will:

- Present the results of the implementation and sustainability of a process management system based on COBIT and its positive impact on the reliability of the enterprise internal control system
- Submit an approach to implementing COBIT 5 as an extension of that operating model by identifying gaps to be closed with the updated practices to promote continuous and sustainable improvement in the governance and management of enterprise IT (GEIT) in the company
- Present the results of a processes maturity assessment, covering capability and performance, made by incorporating the new processes assessment model and how this evaluation allows enterprises to set clear actions for closing gaps to achieve and maintain the expected levels in processes maturity

Background

Ecopetrol focuses on good ethics and transparency. As Colombia’s largest integrated oil company, with about 7,000 direct employees, Ecopetrol is among the top 40 oil companies in the world and the four largest oil companies in Latin America. In
addition to Colombia, which accounts for 60 percent of Ecopetrol’s total production, the company is involved in exploration and production activities in Brazil, Peru and the US (Gulf of Mexico). Ecopetrol is also increasing its participation in bio-fuels considerably.

The Corporate Governance Code of Ecopetrol comprises the best corporate practices needed to preserve the business ethics and the correct administration and control of the company. This enables the company to compete through recognition and respect for the rights of shareholders, investors and other stakeholders based on clear policies for transparency in the management and disclosure of information about the business, which will, in turn, generate greater confidence among stakeholders and the market in general. The internal control system of Ecopetrol is framed within international standards (COSO).

Ecopetrol’s IT function reports to the vice president of innovation and technology. Its responsibility is to govern the IT processes for the company, including strategy, architecture, portfolio, implementation and operation of IT solutions, and provisioning of IT and infrastructure services to support business processes.

DTI and the IT shared services unit (UTI) are responsible for ensuring IT governance and management, respectively. Both have strong organizational structures distributed in a manner that meets the business’s needs related to IT. In addition, the IT function contains a management and architecture unit and an information security unit, which report to the highest level of the IT division to guide the processes related to IT governance, risk and compliance (GRC).

**Why Ecopetrol Chose COBIT**

When choosing COBIT as the proper IT governance framework to integrate an IT management system, DTI did so based on the following characteristics of COBIT:

- Mapping of IT goals to business goals
- Better alignment based on a business focus
- A view of what IT does that is understandable to management
- Indication of clear ownership and responsibilities based on process orientation
- General acceptance by third parties and regulators
- A shared understanding among all stakeholders based on a common language
- Fulfilment of the COSO and US Sarbanes-Oxley Act requirements for the IT control environment

In the last quarter of 2008, Ecopetrol’s IT division defined the guidelines, processes and control objectives to implement. Similarly, the division identified the internal resources that would support the implementation of the system and allocated resources to hire the required external consultants.

The team established a project, giving special consideration to the following issues:

- Addressing resource allocation and creating an interdisciplinary team with representatives from the involved areas within IT
- Defining the points of relationship with business units and other support units and interacting with key areas—finance, risk, strategy, quality, and internal and external audit—on an ongoing basis
- Integrating and converging with the IT support team in transport operations that was anticipating a COBIT implementation effort
- Aligning with business projects—strengthening the internal control system (COSO) and compliance (Sarbanes-Oxley). DTI considered the various business initiatives and ongoing projects to ensure the coordination and integration of efforts.
- Establishing a line of reporting at the highest level of management, with weekly follow-up meetings on the project
- Identifying prior applications (Sarbanes-Oxley, high component in SAP) and others critical for business processes, with equal understanding of the people, resources and infrastructure associated with these applications

Ecopetrol chose to implement 28 COBIT 4.1 processes, giving priority to the control objectives that support Sarbanes-Oxley compliance. The IT division developed an internal exercise to determine the maturity level of these processes. After concluding that they were at an average maturity level of 2, the team identified the gaps and set up action plans to reach level 3 for the most critical processes.

Since the second half of 2009, internal and external annual audits had been developed for Sarbanes-Oxley compliance. Several measures were implemented for remediation and improvement of key IT processes and controls. As a result, the external auditor reported that there were no significant deficiencies or material weaknesses in IT controls that need to be
reported by the chief information officer (CIO), chief financial officer (CFO), chief executive officer (CEO) or auditor.

In December 2009, the COBIT project implementation received a company award for excellence, recognizing the project team’s results, performance, initiative and teamwork. The financial, management and growth results of the company have been internationally recognized during recent years.

From 2009 through the end of 2013, the company showed significant results in the management of IT risk and control, key performance indicators, and internal and external audits and assessments related to maturity of capability and performance in the IT processes.

As part of the challenges of operational excellence, the IT function at Ecopetrol maintained a clear approach toward governance and management of IT services and processes and assesses them based on the best global reference standards and by running ongoing sustainability and optimization actions. Additionally, DTI developed a plan to adopt new versions of practices, such as COSO 2013 and COBIT 5, looking for the consolidation of strong IT governance practices totally aligned with the corporate internal control initiatives.

Key Success Factors
In 2010, the IT function structured a sustainability and optimization plan for its IT management system, based on the premise of having a comprehensive vision, as well as organizational and operating model, and leveraging IT to achieve automation in IT processes and controls.

Ecopetrol also structured the IT compliance area, referencing the good practices of the COBIT framework and integrating the risk management cycles.

Key issues that led to the excellent results of the use of COBIT in Ecopetrol’s IT management system include:

- The use of COBIT was structured as a project with a detailed work plan, clearly defined milestones, allocation of team work with dedication and reliance on project management, risk management, and control of project timing and deliverables.
- The team had the full support of management, provided progress reports, and brought up any deviations and actions that required assurance.
- The company hired well-known, specialized consulting firms that integrated teams with extensive knowledge and experience.
- The project planning, development and results were communicated effectively within the company.
- The appropriation of practices by the process owners and control responsibilities were assured and formalized.
- The project was well integrated, with all areas involved, and synergies were leveraged, especially with the IT support team in transport operations, which provided the results of previous efforts and guaranteed the perspective of business users.
- A community of practice and management of lessons learned were established.
- Sustainability strategies and further optimization of processes were defined.
- The IT function interacted effectively with the audit teams.
- Particular focus was given to segregation of duties, access control, continuity planning, software development and information security issues.
- Maturity level assessments were conducted by a competent and independent third party.
- More than 20 employees passed ISACA’s COBIT Foundation Exam.
- Several employees were or became members of ISACA, which gave them easier access to more detailed guidance.

By 2013, Ecopetrol had updated the design of the IT processes and they had been embedded in the integrated business processes model. This led to important optimizations in transversal activities and propitiating standardization and simplification. Ecopetrol is now extending the practices of its IT governance and COBIT implementation to the companies in its business group.
During the last five years, the IT division contracted with an external consultant to conduct the capability maturity level assessment for the critical IT processes. These annual assessments confirmed the sustainability in the achievement of maturity levels 3 and 4 in the company’s processes, according to the goals. In addition, the IT division has incorporated the principles of the updated COBIT Process Assessment Model (PAM): Using COBIT® 5 to include the assessment not only of the processes’ capability, but also their performance under the ISO 15504 standard.

The results of the most recent assessment reported an average of 3.8 in the capability maturity of the company’s 16 IT processes (figure 1) and an average of 3.6 in the performance maturity of the same processes (figure 2).

Moving Forward With COBIT 5
Aligned with the challenges of growth and operational excellence, commitment to transparency and guaranteeing the reliability of information in its processes and to its stakeholders, the IT function endeavored to extend the IT processes to COBIT 5 by integrating the efforts and ensuring alignment with ongoing corporative initiatives related to the design and implementation of the Shared Services Center (SSC), integration of management processes (business process management [BPM]), enterprise risk management (ERM) and the internal control system (COSO ERM).

With the extension of the control objectives mapped with COBIT 5 practices and the structuring of sustainability and process-based optimization model, Ecopetrol maintains a strong foundation for the sustainability and improvement of its IT processes.

To ensure the alignment and stability of the COBIT 4.1-based system, the strategy has been designed to expand to new management and governance practices and includes the key practical aspects of the integration of COBIT 5 practices to improve the IT GRC capabilities. Through all of this, the stakeholders maintain an understanding that the new practices are broader in scope and the implications of incorporating these practices are an extension of the COBIT 4.1 control objectives that are already implemented on the previous IT processes.

The plan includes mapping items between current processes and COBIT 5 practices to identify gaps to close and also contains an approach to establish a relationship and communication plan to interact with stakeholders and people involved in leveraging the optimization of the IT GRC processes.
Figures 3 through 7 show the evolution of some issues and results related to IT compliance at Ecopetrol:

- IT key controls and their distribution between governance and management units have evolved through the application of optimization, prioritization and rationalization practices. This evolution is also a consequence of processes maturation and integration (figure 3).
- IT key controls compliance reported by ongoing monitoring, before remediation plans and audits, has evolved by the sustainability of the processes (figure 4).
- Audit findings related to design and operation of IT controls, reported before remediation plans, have been decreasing according to the optimization of controls and processes maturation (figure 5).
- Action plans have been developed to cover key findings related to IT controls by ongoing monitoring (figure 6).
- In relation to IT GRC practices, Ecopetrol has adopted best practices and, particularly, global frameworks (figure 7).

**Conclusion**

The implementation and sustainability of GRC processes based on COBIT are very urgent initiatives that imply important efforts, but that propitiate very positive impacts on the reliability of the enterprise internal control system, clearly generating reliable information that supports business strategy.

Implementing COBIT 5 on a processes operating model based on a previous version requires a clear strategy that permits leveraging the newest practices without affecting current results. It could be made by identifying gaps to be closed and considering key issues like communication; it is
necessary to identify and report benefits. This migration promotes the continuous and sustainable improvement in the governance and management of information technology in the enterprise.

The maturity assessment over the processes capability and performance, using the COBIT 5 PAM and referring to ISO 15504, is an important source to validate the achievement of the current maturity level and to identify gaps to set actions to improve the processes maturity in order to accomplish objectives. However, development of these assessments should be permanent and strict in their methodology, the assessor’s competencies and processes owners involvement.

Finally, in the context of COBIT 5’s use and sustainability process, the impact of the results on the information reliability, the strong confidence of IT in the internal control system, the integration with organizational associated issues, the ongoing external assessment, the management of culture and people, and the effective support of consulting services are key success factors.

Alberto León Lozano, CISA, CGEIT, CIA, CRMA
Is IT compliance officer of the information technology division at Ecopetrol S.A. He can be reached at Alberto.Leon@ecopetrol.com.co

©2014 ISACA. All rights reserved.