DISCUSS THIS ARTICLE

4 Steps to Integrate IT and Corporate Governance

By Rodrigo de Grazia Bacha Estevam, PMP, and Joao Souza Neto, Ph.D., CGEIT, CRISC, COBIT Certified Assessor

COBIT Focus | 1 December 2014

In October 2012, the Brazilian Court of Audit (TCU) conducted a survey involving 337 public institutions, and found that in most of the organizations, corporate governance did not include IT governance under its jurisdiction, granting a worrisome autonomy to the IT department.[1]

To deal with this omission, a governance model has been proposed involving the integration of corporate governance with IT governance. The integrated model aims to ensure not only the optimization of internal controls to achieve compliance, transparency and accountability, but also the proper use of investments in IT aligned with corporate strategic objectives.

The integrated model is based on the relationship between King III[2] and COBIT® 5.[3] The explicit relationship between these governance models is based on the principles of the fifth element of King III, IT governance, and in four of the five processes of the Evaluate, Direct and Monitor (EDM) domain of COBIT 5, in which the board of directors is accountable, per the Responsible, Accountable, Consulted and Informed (RACI) matrices.

The implementation of the integrated model may be undertaken in four phases, which are ordered from strategy to IT operation, and are in line with the traditional logical sequencing of the implementation of a governance model.

Phase 1—The Board Gets Involved

The first phase begins with COBIT 5 process EDM01 *Ensure governance framework setting and maintenance*, which is responsible for defining the governance system used by the organization. The process is composed of three governance practices that evaluate, direct and monitor the governance system. All the outputs of these practices are inputs to other processes of the EDM domain, i.e., EDM01 is a prerequisite for the deployment of other EDM processes. This justifies starting the implementation of the model with this process.

EDM01 explicitly references two principles of the King III's IT Governance element: 5.1 "The board should be responsible for information technology governance" and 5.3 "The board should delegate to management the responsibility for the implementation of an IT governance framework."

King III states in principle 5.1 that, "The board shall be responsible for IT governance and put it on its agenda." King III considers IT governance as one of the main references for corporate governance because it provides information to senior management for decision making. Because it is accountable for IT governance implementation, the board must also ensure that IT policies are established and implemented, and it should receive independent assurance on the effectiveness of internal controls. Regarding principle 5.3, King III states that "IT management is responsible for the implementation of IT governance framework structures, mechanisms and processes; an IT committee should be implemented to advise the board; and a chief information officer (CIO) should be appointed to lead IT management in the implementation of the IT governance framework."

Phase 2—Ensure Value Creation

The second phase of the implementation of the integrated governance model is composed of COBIT processes EDM02 *Ensure benefits delivery*, EDM03 *Ensure risk optimization*, and EDM04 *Ensure resource optimization*. All these processes are implemented in parallel, because there are no dependencies between them. These three processes are each related to at least one principle of the IT Governance element of King III.

Process EDM02 is linked to principle 5.2, "IT should be aligned with the performance and sustainability objectives of the organization." The aim of the practices of this principle is to ensure that the IT strategy is aligned with the business strategy of the organization and its processes. In relation to this principle, the board is accountable for establishing processes to identify and exploit opportunities to optimize performance and sustainability of the organization through the use of IT.

Process EDM03, in turn, is related to the principles 5.5, "IT should form an integral part of the company's risk management," and 5.7, "A risk committee and audit committee should assist the board in carrying out its IT responsibilities." The goal of the practices of this principle is the joint engagement of IT and other areas on corporate risk management. The board, on this principle, demands that all legal compliance is integrated with risk management. Principle 5.7 has its practices oriented toward the effectiveness of risk management by risk and audit committees through the appropriate approach to financial and IT risk, among others, and also through the use of IT to improve the efficacy of the audits.

Process EDM04 is related to King III principle 5.6 "The board should ensure that information assets are managed effectively." The goals of the practices of this principle are managing information as an important business asset and ensuring the implementation of strategies and systems for effective information management and information security.

Phase 3—Stakeholder Management

The third phase of the implementation is focused on process EDM05 *Ensuring stakeholder transparency*. The three practices of this process deal with the relationship of IT governance with stakeholders. The first practice, EDM05.01 *Evaluate stakeholder reporting requirements*, focuses on collecting all the requirements necessary to provide information to the stakeholders. The second and third practices, EDM05.02 *Direct stakeholder communication and reporting* and EDM05.03 *Monitor stakeholder communication*, are focused on monitoring and reporting requirements as defined in the first practice.

The management practice EDM05.01 receives inputs from practices EDM02.03, EDM03.03 and EDM04.03, which monitor, respectively, the management of benefits, risk and resources. These inputs are provided for the purpose of communicating information to stakeholders regarding each one of these practices. With these inputs, the requirements are listed and targeted to the stakeholders, as planned.

COBIT process EDM05 is the only process on the EDM domain that has no relation to King III. Even so, King III does have a specific element for the governance of the relationship among the stakeholders of the organization. The integrated model relates the COBIT process EDM05 to King III principle 8.5 "Transparent and effective communication with stakeholders is essential for building and maintaining their trust and confidence." This principle is part of the eighth element of governance of King III, "Governing stakeholders' relationship," and its practices aim for the establishment of an affordable, reliable and transparent communication with all stakeholders, in an appropriate language, according to legal and strategic considerations of the organization. Besides, the board must adopt/develop communication guidelines that support a communication program that meets the expectations of stakeholders.

Phase 4—IT Management Support

The final phase consists of the implementation of COBIT 5 management processes that have the board ranked as "informed" in the RACI chart. This is an essential step to ensure that the board has the proper insight and oversight into management processes that directly support the governance domain.

To keep the implementation sequence initiated in phase 1, the first management processes to be implemented are those that have practices that receive inputs and/or send outputs to EDM practices, as shown in **figure 1**.

Figure 1—Management Practices That Send Inputs and/or Receive Outputs From Practices of the EDM

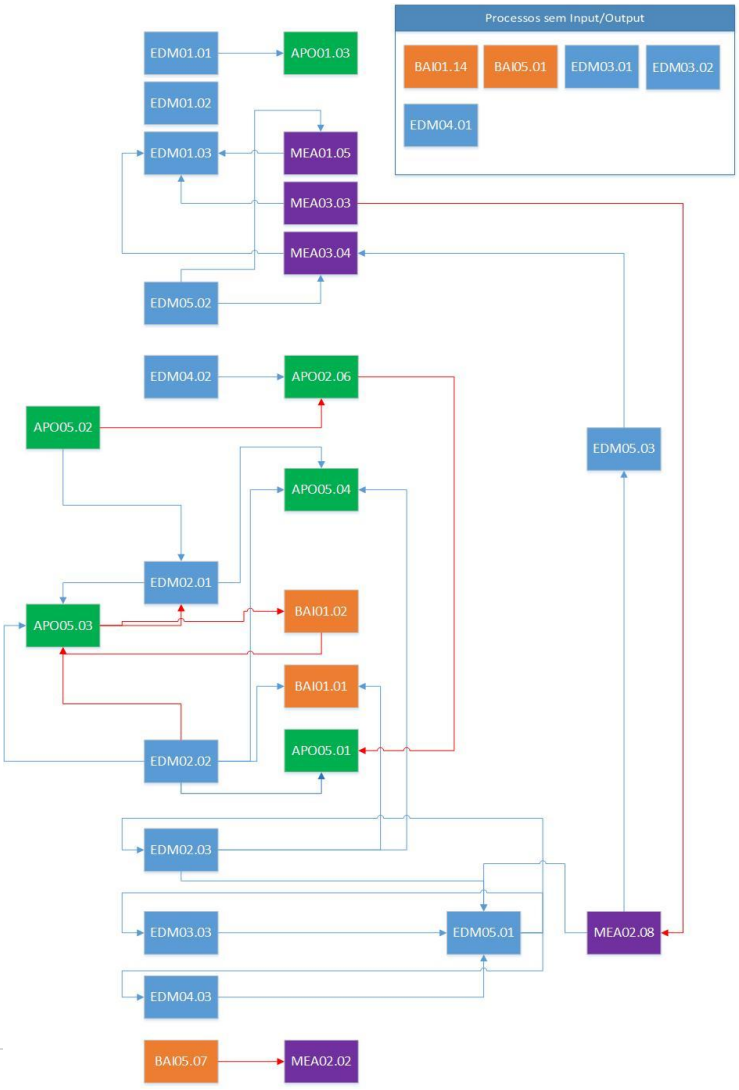
Domain

Practices That Send Inputs	Practices That Receive Outputs
APO05.02	APO01.03
APO05.03	APO02.06
MEA01.05	APO05.01
MEA02.08	APO05.03
MEA03.03	APO05.04
MEA03.04	BAI01.01
	MEA03.04

Figure 2 shows the interconnections between governance practices and management practices involved in the implementation of the integrated governance model.

Figure 2—Interconnections Between Governance Practices and Management Practices

Implementing the Model



Source: Rodrigo de Grazia Bacha Estevam and Joao Souza Neto. Reprinted with permission.

Figure 3 presents a summary of actions per implementation phase to be executed in the IT area and in the bylaws of the board of directors.

Figure 3—Summary of Actions Per Implementation Phase

Phase	Related KING III Principles	IT	Board of Directors
1	5.1 The board should be responsible for Information Technology governance 5.3 The board should delegate to management the responsibility for the implementation of an IT governance framework.	Appoint a CIO to lead IT management in the implementation of the structures, processes and mechanisms for the IT governance framework, implement the process EDM01, and establish an IT strategic committee.	Include in the bylaws of the board of directors: the board is accountable for IT governance; the board should ensure that IT policies are established and implemented, and receive independent assurance on the effectiveness of internal controls.
2	5.2 IT should be aligned with the performance and sustainability objectives of the organization. 5.5 IT should form an integral part of the company's risk management. 5.6 The board should ensure that information assets are managed effectively. 5.7 A risk committee and audit committee should assist the board in carrying out its IT responsibilities.	Implement the processes EDM02 *Ensure benefits delivery*, EDM03 *Ensure risk optimization*, and EDM04 *Ensure resource optimization*. The CIO should ensure that IT is aligned with the goals of performance and sustainability of the organization.	Include in the bylaws of the board that it is accountable for establishing that: there are processes to identify and exploit opportunities to optimize performance and sustainability of the organization through the use of IT; the entire corporate legal compliance is integrated with risk management; the risk and audit committees strive for the effectiveness of risk management; IT assets are managed effectively, ensuring that strategies and systems for the effective management of information and information security are implemented.
3	8.5 Transparent and effective communication with stakeholders is essential for building and maintaining their trust and confidence.	Implement practices EDM05.01 *Evaluate stakeholder reporting requirements*, EDM05.02 *Direct stakeholder communication and reporting*, and EDM05.03 *Monitor stakeholder communication*.	Implement guidelines for establishing a communications program with stakeholders, to increase trust and confidence between stakeholders and the organization.
4	None	Implement practices: APO05.02, APO01.03, APO05.03, APO02.06, MEA01.05, APO05.01, MEA02.08, APO05.03, MEA03.03, APO05.04, MEA03.04, BAI01.01, and MEA0304.	Implement management practices that have the board of directors included in the RACI Chart.

The step-by-step process shows that the implementation of an integrated governance model based on King III and COBIT 5 is viable. Activities were described for adapting the board's bylaws and for the implementation of COBIT 5's practices, aiming to ensure not only the optimization of internal controls to achieve compliance, transparency and accountability, but also the proper use of investments in IT aligned with corporate strategic objectives.

Rodrigo de Grazia Bacha Estevam, PMP

Is a specialist in computer networks with more than 12 years of experience managing IT and more than 10 years as a project manager in IT projects.

Joao Souza Neto, Ph.D., CGEIT, CRISC, COBIT Certified Assessor

Has more than eight years of experience in IT governance, applying COBIT within Brazil Post. He is also responsible for the IT governance research area in the Universidade Catolica de Brasilia. He is founder and institutional director of the ISACA Brasilia (Brazil) Chapter.

Endnotes

[1] Tribunal de Contas da Uniao, "Relatorio do Levantamento de Governança de TI 2012," 5 November 2012, *www.aneel.gov.br/arquivos/PDF/igovti2012.pdf*

[2] Institute of Directors in South Africa (IDSA), King Report on Corporate Governance (King III), South Africa, 2009, p. 64

[3] ISACA, **COBIT 5**, USA 2012, p. 94