> DISCUSS THIS ARTICLE

COBIT Helps Organizations Meet Performance and Compliance Requirements

By Sreechith Radhakrishnan, COBIT Certified Assessor, ISO/IEC 20000 LA, ISO/IEC 27001 LA, ISO22301 LA, ITIL Expert, PMP

COBIT Focus | 6 April 2015 English

Many organizations need help meeting performance and compliance requirements. A consulting company in the United Arab Emirates worked with three different organizations to help each organization meet its governance, risk and compliance (GRC) requirements. The organizations included a government organization (5,000-plus employees with 170-plus IT staff members), a large financial institution (8,000-plus employees, operating in 3 countries with 250-plus IT staff members) and a large conglomerate (25,000-plus employees, operating in 10 countries with 200-plus IT staff members).

The consultancy determined that the best way to help these clients move from where they were to meeting GRC requirements was by using **COBIT® 5**. **Figure 1** indicates the requirements from the clients and why COBIT 5 was determined to be the best framework to employ.

Figure 1—Why Use COBIT 5?

Requirements From Client	**Why COBIT?**
Clients are using multiple frameworks and standards including ITIL®, ISO/IEC 20000, ISO/IEC 27001, Capability Maturity Model Integration (CMMI®), Enterprise Architecture and Project Management Institute (PMI) Methodology to manage their IT. Individual functions within IT operated in silos and focused on their own framework/standard.	COBIT 5 is aligned with all these frameworks and standards. By using the COBIT 5 framework, the organization can have overall visibility on the performance. The dependencies of each function are clearly visible when COBIT 5 is used as an integrated model.
There are regulatory compliance requirements from local government and authorities. There are audit findings from regulators for	COBIT 5 supports compliance requirements including information security and risk management. COBIT 5 also helps to narrate an organization's

internal controls.	internal controls (in COBIT 5 practices).

Source: Global Success System FZ LLC. IT Domain mapped to COBIT Processes. Reprinted with permission.

Each organization had priorities that needed to be addressed. Some of the more critical issues common to all 3 organizations were:

- Meeting regulatory compliance requirements
- Performing end-to-end IT process capability assessments to identify strengths, weaknesses and areas in need of improvement
- Developing IT risk management frameworks
- Most important, the need to bring all the individual functions within IT into a common, integrated model

One of the organizations had been using COBIT 4.1 for 3 years, and migrating to COBIT 5 was also part of the requirement.

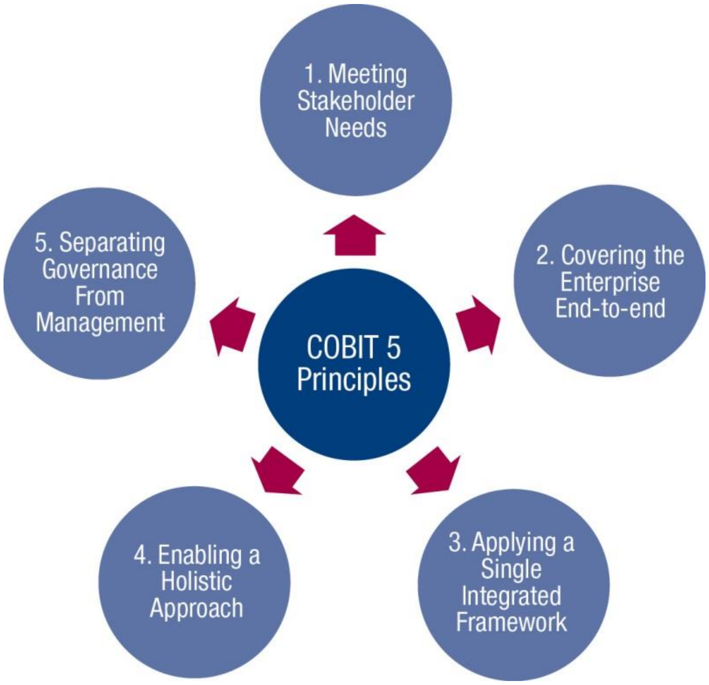
COBIT 5's process guidelines and capability assessment model, along with COBIT 4.1 and Risk IT, were used to meet the clients' needs.

Getting Support From Management

Stakeholders know that implementing critical changes in any organization requires the understanding and support of senior management. In these cases, that support was crucial. Support from senior management was obtained by identifying the business pain areas and mapping those to COBIT to explain the need for control-driven IT.

The organizations also used COBIT 5's goals cascade mechanism to explain how these projects would better align with business objectives. The organizations demonstrated the importance of a holistic approach—one of the COBIT 5 principles (**figure 2**)—to improve the performance of IT.

Figure 2—COBIT 5 Principles


1. Meeting Stakeholder Needs
2. Covering the Enterprise End-to-end
3. Applying a Single Integrated Framework
4. Enabling a Holistic Approach
5. Separating Governance From Management
COBIT 5 Principles

Source: ISACA, **COBIT 5**, USA, 2012

Each organization had similar goals. Each needed to implement a common vocabulary among all IT functions—to meet the performance needs of the business and achieve regulatory compliance and audit requirements.

COBIT was identified as the framework to meet the goals of the organizations, and its goals cascade was used to identify the right processes.

Achieving the Goals

In each case, the organizations used the same approach to achieve their stated goals. First, they performed an initial process capability assessment to identify their strengths, weakness and risk. From there, the most important processes and controls (practices) on which to improve and focus were selected. Priority was given to compliance and audit requirements. A road map was then developed to improve the processes (short-term and long-term projects).

For each organization, the improvement journey started with developing Responsible, Accountable, Consulted and Informed (RACI) charts to assign roles and responsibilities, documenting policies and procedures. More focus was given to organizational change management through awareness sessions, train-the-trainer sessions for key personnel and frequently reviewing progress.

Figure 3 shows an example of how a specific process or issue was addressed and improved. The project management and systems development life cycle (SDLC) improvements were mapped to COBIT 5 processes and control objectives.

Figure 3—Mapping Program and Project Management to COBIT Processes and Control Objectives

Domain	Process ID	Process Description
Program and Project Management	APO06	Manage budget and costs
	APO07	Manage human resources
	APO08	Manage relationships
	APO10	Manage suppliers
	BAI01	Manage programs and project
	BAI02	Manage requirements definition
	BAI03	Manage solutions identification and build
	BAI06	Manage changes
	BAI07	Manage change acceptance and transitioning
	DSS01	Manage operations
	MEA01	Monitor, evaluate and assess performance and conformance

Source: Global Success System FZ LLC. IT Domain mapped to COBIT Processes. Reprinted with permission.

Regulatory compliance requirements were also mapped to COBIT processes and controls (**figure 4**).

Figure 4—Mapping Regulatory Compliance Requirements to COBIT Processes and Control Objectives

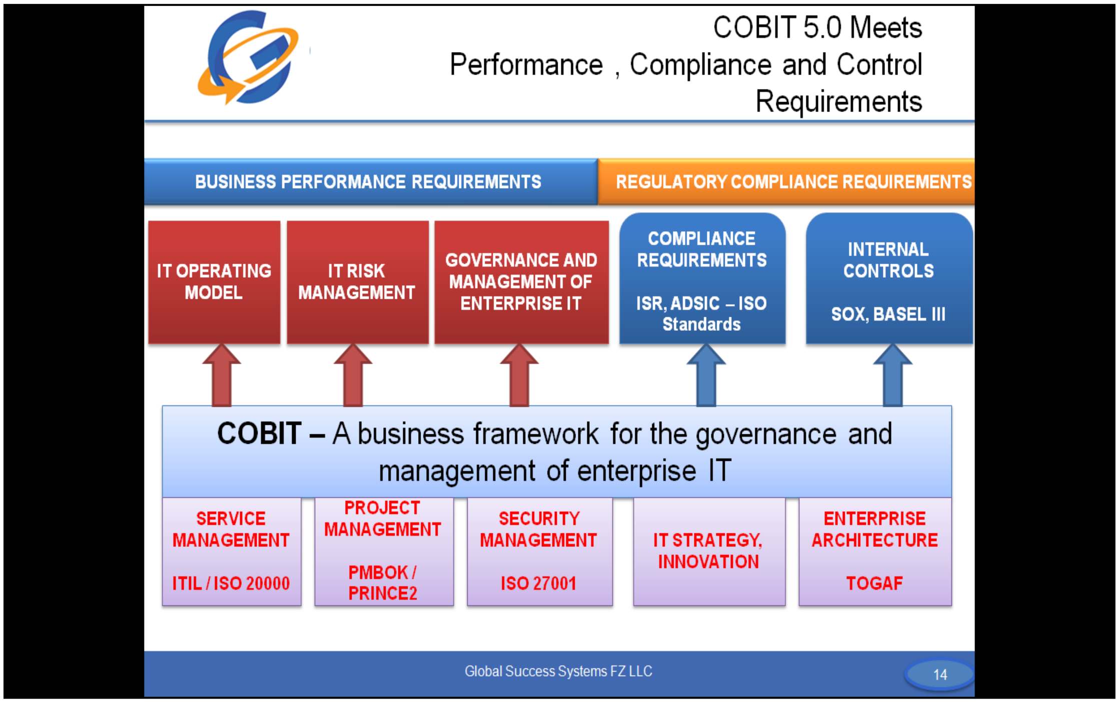
Domain	Process ID	Process Description
Information Security Regulations	APO13	Manage security
	BAI09	Manage assets
	APO12	Manage risk
	DSS02	Manage service requests and incidents
	DSS03	Manage problems
	DSS05	Manage security services
	DSS01	Manage operations
	APO01	Manage the IT management framework
	DSS04	Manage continuity
	BAI01	Manage programs and projects
	BAI02	Manage requirements definition
	BAI03	Manage solutions identification and build
	BAI07	Manage change acceptance and transitioning
	DSS05	Manage security services
		Process RACI charts, organization structure
	MEA01	Monitor, evaluate and assess performance and conformance
	MEA02	Monitor, evaluate and assess the system of internal control

Source: Global Success System FZ LLC. Regulatory Compliance Requirements mapped to COBIT Processes. Reprinted with permission.

As a result, a model (**figure 5**) was produced, from which COBIT can be used to meet the IT performance and compliance requirements of the clients.

This single integrated model helps the organizations to prioritize their goals and choose the right processes and practices to meet their IT performance and regulatory compliance requirements.

Figure 5—Meeting IT Performance, Audit and Compliance Requirements Model



COBIT 5.0 Meets
Performance , Compliance and Control
Requirements

BUSINESS PERFORMANCE REQUIREMENTS

REGULATORY COMPLIANCE REQUIREMENTS

IT OPERATING MODEL

IT RISK MANAGEMENT

GOVERNANCE AND MANAGEMENT OF ENTERPRISE IT

COMPLIANCE REQUIREMENTS

ISR, ADSIC – ISO Standards

INTERNAL CONTROLS

SOX, BASEL III

COBIT – A business framework for the governance and management of enterprise IT

SERVICE MANAGEMENT

ITIL / ISO 20000

PROJECT MANAGEMENT

PMBOK / PRINCE2

SECURITY MANAGEMENT

ISO 27001

IT STRATEGY, INNOVATION

ENTERPRISE ARCHITECTURE

TOGAF

Global Success Systems FZ LLC

14

Source: Global Success System FZ LLC. Integrated IT Performance and Compliance Model. Reprinted with permission.

Conclusion

COBIT can be used by every organization to improve IT performance. It is not a one-size-fits-all model, so understanding the stakeholder needs and business challenges and then utilizing the goals cascade guidelines (enterprise goals > IT goals > enabler goals) is not only important, but extremely helpful and productive. It is always critical to gain senior management buy-in by showing the business benefit of using the COBIT framework.

One of the keys to successful implementation is choosing the required controls (key practices) rather than blindly following the framework and implementing the process. Ensuring that roles and responsibilities within an organization are clearly defined and shared with the team (using RACI charts) is also critical. Dividing the improvement project into small phases helps keep the project going as the organization continues to reap the benefits, and ISACA's ***COBIT® 5 Implementation*** can be used to assist with this.

The process of adopting the COBIT framework is well supported with a number of available guides from ISACA®, but at the same time, one should not hesitate to seek help from experts. And, remember to focus more on people rather documentation. Documentation is not the implementation. It is about people and educating them to behave in a new way.

Sreechith Radhakrishnan, COBIT Certified Assessor, ISO/IEC 20000 LA, ISO/IEC 27001 LA, ISO22301 LA, ITIL Expert, PMP

Is lead trainer and principal consultant with Global Success Systems FZ LLC, United Arab Emirates, where he and his team help organizations improve their IT performance and reap maximum benefit from their IT investments. He is the world's first COBIT 5 Certified Assessor. He is an accredited trainer for multiple disciplines including COBIT, ITIL, PMP and IT Security. He has more than 19 years of dynamic IT management experience including network infrastructure management, project management, IT operations management and service management.