

## How to Start a CobiT Deployment

**Bill Malik**

Control Objectives for Information and Related Technology (CobiT) can help the infrastructure and operations (I&O) management team to clarify workflow, data ownership, process ownership, skill requirements, defect causes and technology applicability. By mapping I&O work into CobiT processes, leadership can improve quality, reduce costs and simplify business procedures.

### Key Findings

- CobiT is much more than an audit standard. It is a comprehensive process model for describing and governing the primary tasks involved with running an IT operation.
- Ultimately, the best way to deploy CobiT is to define your desired state and adapt CobiT to meet your specific organizational needs.
- Smaller organizations can obtain many of the benefits of CobiT through the Quickstart method.
- Larger organizations can use the Quickstart method to initiate a CobiT deployment, but should plan to complete the full CobiT implementation to achieve comprehensive process transparency and quality improvements.
- IT process frameworks, such as CobiT, Information Technology Infrastructure Library (ITIL), and International Organization for Standardization (ISO) 20000, help IT organizations improve efficiency.

### Recommendations

- If you are seeking to optimize constrained I&O resources against growing demand for service, then IT process frameworks like as CobiT and ITIL can eliminate sources of error and waste.
- Use the CobiT process maturity indicators in conjunction with the I&O Maturity Model to assess your IT organization's capabilities and optimal next steps.
- Define I&O jobs in CobiT terms to visually and unambiguously link skills, processes, workflow and technology.
- Enhance the governance of the IT organization by mapping information flows in the IT organization using the CobiT process model.

## **STRATEGIC PLANNING ASSUMPTION(S)**

---

By 2014, more than 8% of large enterprises globally will have adopted some form of CobiT as an IT process management framework.

## **ANALYSIS**

---

Many organizations may see CobiT primarily as a tool for auditors. Its use in the IT audit community is broad. However, CobiT also offers more direct value to the I&O leadership team, and it can serve as a process model for the IT organization, covering all phases of the procurement, development and production environment. As such, it helps organizations clarify reporting relationships, process linkages across teams, and data flows within and across the IT organization, and it can help identify structural problems. For instance, if one team manages pieces of multiple CobiT processes, then the organization may find that that team generates a disproportionate number of quality problems. Furthermore, if one team owns multiple CobiT processes, then the organization may be at risk of violating separation of duties' controls for those processes. However, the benefit of structuring the IT organization's processes along CobiT lines (and this also applies ITIL and other IT process frameworks; see Note 1) is that the organization can clearly understand process inter-relationships and data paths, allowing the organization to eliminate unnecessary process steps and optimize processes. This can yield substantial improvements in operational quality and efficiency, driving down costs through eliminating wasted or redundant effort.

This research discusses how an I&O organization can deploy CobiT, using the CobiT process model to describe the activities performed by the staff in the I&O organization. The core issue of this research is where to start. Because CobiT is used by some IT auditors, one natural starting place would be to review the CobiT audit findings and address specific deficiencies or suggestions, working to resolve those first. However, if the organization has not had such an audit, then it will need a different approach.

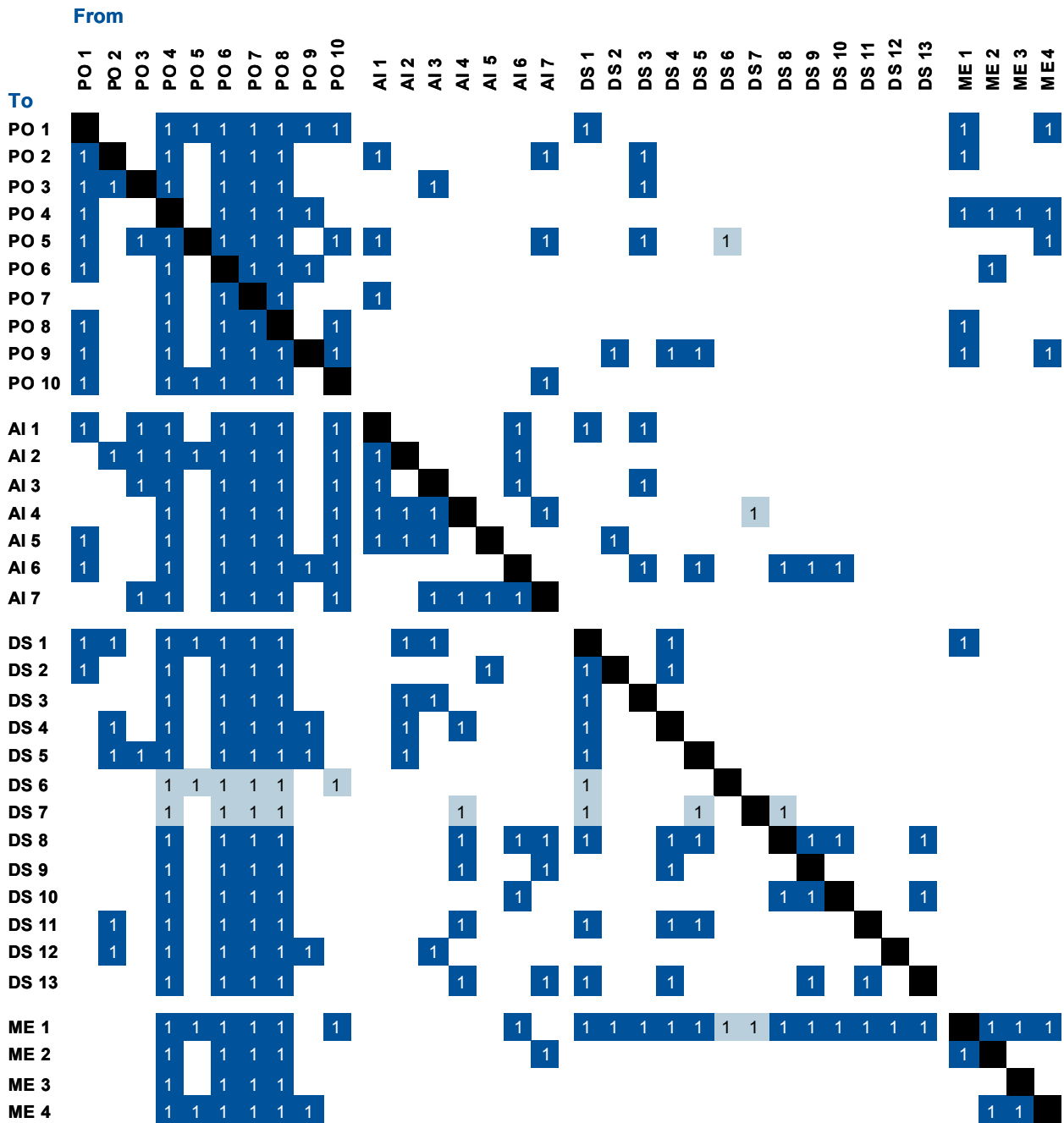
Although there is no one correct answer for all organizations, there are some common practices that support successful CobiT deployments. The first is to start with an area that is currently well-defined. CobiT consists of four domains: plan and organize, acquire and implement, deliver and support, and monitor and evaluate. These domains contain a total of 34 processes and 210 control objectives across these processes. Mapping the roles and processes in the I&O organization into the specific domains and processes can be a daunting task. Smaller organizations may not have sufficient staff to deploy the full CobiT suite of control objectives; for them, the IT Governance Institute (ITGI; [www.itgi.org](http://www.itgi.org)) has defined a subset of CobiT called Quickstart, which contains 32 processes and 59 control objectives. Note that, for large enterprises, Quickstart does not provide as comprehensive a set of controls as full CobiT; however, it may be useful as a starting point for a comprehensive CobiT deployment.

Of the four domains, organizations will be better at some than at others. Because most organizations are (statistically speaking) at Level 1 or Level 2 in terms of their I&O process maturity, most of them would tend to do better at activities in the delivery and support domain. This domain contains the processes typically associated with running the data center. Other organizations that have spent a good deal of effort improving their application development skills may be superior in the acquire and implement domain, which contains the processes for transforming a business requirement into a working software product.

Organizations with strong delivery and support capabilities should begin by formalizing their define and manage service levels (DS1) capabilities, which provide input to a dozen CobiT

processes. Once that domain is well-defined, the next-most-important processes are: ensure continuous service, with eight dependent processes (DS4); manage performance and capacity (DS3), with seven dependent processes; ensure system security (DS5), with six dependent processes; and manage the configuration (DS9), with five dependent processes. Figure 1 offers a depiction of the relationships between these processes. (Outputs from the processes, which are listed along the top, are inputs to the processes listed below. Processes DS6 and DS7 are in a lighter color because they are not included in the Quickstart version of CobiT.) See Note 2 for a complete list of the processes.

Figure 1. CobiT Process Dependencies



Source: Information Systems Audit and Control Association (ISACA)

In the acquire and implement domains, all processes are relatively similar in the number of dependent processes. Procure IT resources (AI5) has only two dependent processes; the rest all provide input to about six other dependent processes. Organizations that are particularly good at these processes may choose to begin their CobiT deployment by documenting their acquire and implement processes, then follow the outputs from these processes as they flow into other I&O

domains. Choose among those dependent processes for the next-candidate processes for transformation into the CobiT model.

Organizations with no clear starting place should begin with the plan and organize domain disciplines. Define a strategic IT plan (PO1) is foundational for the lead activities in all other CobiT domains. Once that is defined, define the IT processes, organization and relationships (PO4); communicate management aims and direction (PO6); manage IT HR (PO7); and manage quality (PO8) each provide input to all other CobiT processes. Manage projects (PO10) provides input to 13 disciplines, most of which are in the acquire and implement domain.

Because all CobiT disciplines provide input to at least one other discipline, and receive input from at least one other discipline, a complete CobiT deployment requires the organization to deploy all disciplines. Until the organization completes that job, some disciplines will not have all the inputs from CobiT-defined processes. On the receiving side, monitor and evaluate IT performance (ME1) takes input from 23 processes, and manage service desk and incidents (DS8) receives input from 13 processes. Manage the IT investment (PO5) and manage changes (AI6) both read from 12 processes, while assess and manage IT risks (PO9) and define and manage service levels (DS1) read from eleven processes. Define a strategic IT plan (PO1), manage operations (DS13) and all remaining acquire and implement disciplines read from 10 processes, with the exception of acquire and maintain technology infrastructure (AI3), which reads from nine processes. All the other disciplines read input from six to eight sources, except manage IT HR (PO7) and ensure compliance with external requirements (ME3), which only read from four sources. The disciplines that do not have formal CobiT-defined inputs must make do with existing data sources until those sources can be formalized.

## How Much CobiT?

Some firms have gone as far as developing individual job descriptions based on specific CobiT process steps. The HR team develops CobiT-style job descriptions, personnel requisitions are developed to support CobiT process elements, and the employee's performance evaluation references the specific tasks and process maturity associated with those tasks. This yields the benefit that every task and every process has a formal, complete discussion of its required inputs, the tasks to be performed, where the outputs go next, and how the tasks are supervised or governed. There is a spectrum of oversight that ranges from training and supervision through management to governance; depending on the degree of granularity, CobiT can provide a context to support each of these activities.

ISACA has certified over 60,000 CobiT-trained certified information system auditors (CISAs) globally. ISACA does not keep statistics on organizations that are using CobiT as an IT process framework. While ITIL remains the most widely deployed IT process framework, we expect that, by 2014, more than 8% of large enterprises globally will have deployed some form of CobiT as an IT process management framework.

## Bottom Line

The goal of a CobiT deployment is not merely following an abstract model. An effective IT process model defines all the processes necessary to run a data center. Organizations that run data centers perform all these activities, but few have made their processes as explicit as CobiT, ITIL and ISO 20000; therefore, the implementation may be suboptimal. Very few organizations may have built an explicit IT process model on their own. In all cases, the goal is to make implicit processes explicit. Explicit, transparent processes allow the business to tune and optimize those activities, thus eliminating waste, avoiding bottlenecks and delivering what the business needs at a cost it is willing to pay. The best way to deploy CobiT is to define your current state and your

desired state, and to apply CobiT to optimally meet your organization's most-pressing, specific business needs.

## **RECOMMENDED READING**

---

CobiT 4.1 Executive Summary and Framework, ISACA, [www.isaca.org](http://www.isaca.org)

CobiT Quickstart Second Edition, ISACA, [www.isaca.org](http://www.isaca.org)

"Introducing the Gartner IT Infrastructure and Operations Maturity Model"

### **Note 1 Which Process Framework?**

CobiT, owned by ISACA, discusses in detail the main processes that IT organizations use to run data centers. This framework aims to be comprehensive, and supplements each process description with key performance indicators, key goal indicators and a set questions to assess the process maturity of the specific implementation.

ITIL, released by the U.K. Office of Government Commerce (OGC; [www.ogc.gov.uk](http://www.ogc.gov.uk) ), enables IT organizations to take a service life cycle view. It is the most widely deployed IT service management framework.

ISO 20000, based on BS15000 and released by the ISO, is the original IT service management framework. The OGC committed to maintaining alignment between future versions of ITIL and ISO 20000.

From a risk perspective, the choice between these frameworks is less significant than the decision to use any one of them. ISACA has produced guidelines that map many IT process framework standards against CobiT.

### **Note 2 Who Owns CobiT?**

The ITGI is the sister organization to the ISACA. ITGI owns the CobiT and Val-IT process models and related certifications.

The full list of CobiT processes includes:

- PO1: Define a strategic IT plan.
- PO2: Define the information architecture.
- PO3: Determine technological direction.
- PO4: Define the IT processes, organization and relationships.
- PO5: Manage the IT investment.
- PO6: Communicate management aims and direction.
- PO7: Manage IT human resources.
- PO8: Manage quality.
- PO9: Assess and manage IT risks.

- PO10: Manage projects.
- AI1: Identify automated solutions.
- AI2: Acquire and maintain application software.
- AI3: Acquire and maintain technology infrastructure.
- AI4: Enable operation and use.
- AI5: Procure IT resources.
- AI6: Manage changes.
- AI7: Install and accredit solutions and changes.
- DS1: Define and manage service levels.
- DS2: Manage third-party services.
- DS3: Manage performance and capacity.
- DS4: Ensure continuous service.
- DS5: Ensure systems security.
- DS6: Identify and allocate costs.
- DS7: Educate and train users.
- DS8: Manage service desk and incidents.
- DS9: Manage the configuration.
- DS10: Manage problems.
- DS11: Manage data.
- DS12: Manage the physical environment.
- DS13: Manage operations.
- ME1: Monitor and evaluate IT performance.
- ME2: Monitor and evaluate internal control.
- ME3: Ensure compliance with external requirements.
- ME4: Provide IT governance.

## REGIONAL HEADQUARTERS

---

### **Corporate Headquarters**

56 Top Gallant Road  
Stamford, CT 06902-7700  
U.S.A.  
+1 203 964 0096

### **European Headquarters**

Tamesis  
The Glanty  
Egham  
Surrey, TW20 9AW  
UNITED KINGDOM  
+44 1784 431611

### **Asia/Pacific Headquarters**

Gartner Australasia Pty. Ltd.  
Level 9, 141 Walker Street  
North Sydney  
New South Wales 2060  
AUSTRALIA  
+61 2 9459 4600

### **Japan Headquarters**

Gartner Japan Ltd.  
Aobadai Hills, 6F  
7-7, Aobadai, 4-chome  
Meguro-ku, Tokyo 153-0042  
JAPAN  
+81 3 3481 3670

### **Latin America Headquarters**

Gartner do Brazil  
Av. das Nações Unidas, 12551  
9º andar—World Trade Center  
04578-903—São Paulo SP  
BRAZIL  
+55 11 3443 1509