COBIT® Focus
Using COBIT® Val IT™, Risk IT, BMIS™ and ITAF™

In This Issue:

- COBIT for IT Risk Management in a Bank—A Case Study, by Jitendra Barve, CISA, FCA
- Laugh & Learn: Using COBIT to Improve the Software Development Life Cycle, by Corjan Bast
- Using COBIT and COSO ERM, by Christopher Fox, ACA
- Mapping FFIEC Framework With COBIT 4.1, by Kenny Lee, CISA, CISM, CISSP
- New COBIT Case Study: Ecopetrol S.A.

COBIT for IT Risk Management in a Bank—A Case Study
By Jitendra Barve, CISA, FCA

This case study is a real-life example of using COBIT® for IT risk management within a global bank. COBIT was used effectively for managing risk within the technology teams to ensure that appropriate IT governance and IT assurance processes were utilised throughout the bank.

Background
The bank in the given case is a global conglomerate with operations in more than 50 countries and with more than 125,000 employees across the globe. The bank’s technology teams are located throughout the world to support global lines of business. The IT teams include development centres that are part of the bank and others that are outsourced to vendors, as well as technology back offices that support IT infrastructure and services. The bank had a history of multiple governance and assurance templates and processes followed by different teams, regions and locations. Hence, the key challenge was to create a common governance and assurance process across technology teams.

The technology governance and assurance programme was designed through a risk management framework to ensure effective risk and control management.

The framework was defined to address existing risk and control management weaknesses, such as:
- Immature processes for assessing and testing compliance
- Lack of a single control repository, resulting in control duplication
- Lack of a clear, repeatable process for completing risk assessments

The new framework was expected to enable technology teams to understand the significant operational risks and their impact on the wider organisation by:
- Addressing areas in which risks were not effectively controlled
- Allowing technology executives to demonstrate regulatory responsibilities efficiently
- Using a common platform for reporting all regulatory requirements across regions and countries
- Effectively reporting technology risk and control weaknesses that may impact the business

Call for Articles

How are you using COBIT®, Val IT™, Risk IT, BMIS™ or ITAF™ at your enterprise?
Submit articles on your experiences with these frameworks.
Deadline to submit copy for volume 4, 2010:
10 September
Submit articles for peer review to:
publication@isaca.org
• Implementing a standard process across regions and offices to ensure consistency and avoid duplication of reporting

Use of COBIT
The governance team decided to use COBIT as a standard framework. A team of professionals—including risk, IT security and US Sarbanes-Oxley Act process experts—was set up to define the processes and templates. The team primarily worked on three areas:
1. **Defining a framework to use**—Control objective framework (COF)
2. **Identifying a standard definition of ‘entities’ against which risks and controls were to be evaluated**—Key entity management model
3. **Identifying a risk management process**—Risk and control assessment (RCA)

Key steps in the process of developing a new risk management framework are described in the following sections.

Step 1—Defining COF
The COF was defined to link risks affecting technology offices and industry standard best practice controls as defined by COBIT. Three objectives were set whilst defining the COF:
1. It should act as a tool to facilitate the effective assessment of risks and controls within technology.
2. It should act as a reporting framework to demonstrate how technology satisfies reporting regulatory requirements, including those of Sarbanes-Oxley.
3. It should act as an aid to drive management assurance.

The steps in implementing COF using COBIT included:
• **Identify principal risks**—The principal risks of level I were defined and frozen based on earlier information. Those identified included risks related to technology, operations, people, legal and regulatory, financial reporting, financial crime, brand, and change.
• **Identify level II risks**—The principal risk was further broken down into level II risks. As an example, the ‘technology principal risk’ was further drilled down to:
  - Inadequate design/testing of IT systems
  - Unavailability of IT systems
  - Lack of IT security

<table>
<thead>
<tr>
<th>Inadequate Design/Testing of IT Systems</th>
<th>Non-availability of IT Systems</th>
<th>IT Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>• PO2 Define the information architecture</td>
<td>• AI2 Acquire and maintain application software</td>
<td>• PO2 Define the information architecture</td>
</tr>
<tr>
<td>• PO3 Determine technological direction</td>
<td>• AI3 Acquire and maintain technology infrastructure</td>
<td>• PO4 Define the IT processes, organisation and relationships</td>
</tr>
<tr>
<td>• PO8 Manage quality</td>
<td>• AI5 Procure IT resources</td>
<td>• PO9 Assess and manage IT risks</td>
</tr>
<tr>
<td>• PO10 Manage projects</td>
<td>• DS1 Define and manage service levels</td>
<td>• AI2 Acquire and maintain application software</td>
</tr>
<tr>
<td>• AI1 Identify automated solutions</td>
<td>• DS3 Manage performance and capacity</td>
<td>• DS5 Ensure systems security</td>
</tr>
<tr>
<td>• AI2 Acquire and maintain application software</td>
<td>• DS4 Ensure continuous service</td>
<td>• DS11 Manage data</td>
</tr>
<tr>
<td>• AI3 Acquire and maintain technology infrastructure</td>
<td>• DS8 Manage service desk and incidents</td>
<td>• DS12 Manage the physical environment</td>
</tr>
<tr>
<td>• AI6 Manage changes</td>
<td>• DS10 Manage problems</td>
<td>• DS13 Manage operations</td>
</tr>
<tr>
<td>• AI7 Install and accredit solutions and changes</td>
<td>• DS11 Manage data</td>
<td></td>
</tr>
</tbody>
</table>

**Figure 1—Mapping Level II Risks**

Prior to implementing this framework, each entity, organisation and location had its own set of controls. COBIT helped in developing and managing a single list of controls for each type of risk through the mapping of needed

**Benefit of Step 1**
Prior to implementing this framework, each entity, organisation and location had its own set of controls. COBIT helped in developing and managing a single list of controls for each type of risk through the mapping of needed
controls to COBIT. In turn, this assisted with the attestation of each type of risk, which provided confidence to senior executives on the reporting and attestation process. Subsequently, a risk assessment process was developed to define risks and controls. This helped in ensuring that adequate controls were deployed to cover the principal risks and level II risks.

Step 2—Identifying Entities for Managing Risks and Controls

The key entity management model was defined to include IT building blocks, against which risk and control assessments were to be performed. The IT building blocks are logically linked together for reporting purposes to provide a risk and control assessment for all supporting services within the purview of the technology office.

The IT building blocks were defined as:

- **Process entities**—These represent the processes used to support, control and manage the IT environment. Any control issues in a process entity would affect many IT services, e.g., change control is pervasive across most IT services.
- **Supporting services entities**—Linking with process and technology entities allows for a complete end-to-end risk and control assessment for that supporting service, e.g., interfacing risks amongst technology entities, service-level risks for end-to-end IT service, and integration risks (the management of handoffs between departments).
- **Technology entities**—These represent the ‘traditional’ IT components, e.g., servers, applications, networks and firewalls. The service maps and the RCA process were used to facilitate the identification of the key technology entities that make up each supporting service.
- **Project entities**—Whilst project entities have no effect on the top 20 services, it is very important to capture any control and risk information ahead of go-live. This will allow the target state controls for a new development/project change to be assessed, reported and communicated prior to go-live. Some examples of the top 20 services include ATM connectivity and core banking application support services.

The bank’s method for defining IT services is through an IT service catalogue. As part of its IT service catalogue, each of the top 20 services was identified for the supporting services that underpin it. A service map was created for each supporting service. The service maps illustrate the technology components that are linked together to support the end-to-end services.

Each process entity and technology entity is distinct and can be linked to multiple supporting services. As a result, the key entity management model is flexible and can support expansion to additional IT services as required. The linkage amongst entities allows risk assessments to be aggregated to provide an end-to-end service risk profile, which is meaningful to management and the different clusters managing the entities in the overall service.

**Benefit of Step 2**

Prior to implementing the new risk management process, each region, country, etc., of the bank had its own risk and control matrices. The risk and controls evaluation was based on the understanding of each team working on risk management within the region, and there was no focus on the ‘end result’, i.e., the impact of risk on customer service. COBIT helped in identifying key services that had an impact on business and customers and kept the focus on controls. Once such risks were identified, the controls were frozen based on the COBIT framework and were evaluated for control effectiveness—with the clear objective of determining the impact on customer service. This resulted in reducing the total number of incidents and reducing the impact of incidents on customers and/or customer services.

Step 3—Defining and Implementing the RCA Process

The process overview in **figure 2** highlights the five steps to performing a risk assessment. Within each of the steps, the key tasks were identified. A series of tools/process aides was defined to assist with the scoping, scheduling and delivery of the risk assessment, and is outlined in **figure 2**.

The objective in developing the common RCA process was to ensure that the analyses of risks and controls were consistent across the teams globally.

One of the tools was a simple Excel template defined to capture risk and control information. The template then was frozen for use by all of the entities. The template was defined to capture the following key information:

- Principal and level II risks
- Control objectives with reference to the COBIT controls process
- Reference to Sarbanes-Oxley control requirements
- Control owner
- Control assessment—effective, ineffective
The templates were filled by the risk and control owner and were sent to the central risk team for review. They were then entered into the risk management tool to track actions for closure and reporting on open risks. Each was tagged with:

- **Entity owners**—Typically the owners of the RCA
- **Risk owners**—The owners responsible for the risk
- **Control owners**—The owners responsible for maintaining control effectiveness
- **Action owners**—The owners of actions defined due to ineffective controls

**Benefit of Step 3**
Through training programs, the terms 'entity/RCA owners', 'risk owners', 'control owners' and 'action owners' were explained using a Responsible, Accountable, Consulted and Informed (RACI) chart (see figure 3 for an example). The responsibilities were also mapped in the job descriptions and in performance evaluation criteria of the staff.

The example in figure 3 clarifies that, although the head of facilities was held accountable for providing physical security on an ongoing basis, the chief operations officer (COO) was accountable for ensuring reporting of incidents and follow-up thereof. For any actions of employees and vendor staff working out of the office, human resources (HR) was consulted and informed.

**Step 4—Training Key Stakeholders**
One of the main challenges was to explain the entire process to all of the stakeholders with different roles.

---

### Figure 2—RCA Process Steps

<table>
<thead>
<tr>
<th>Engage</th>
<th>Prepare</th>
<th>Evaluate</th>
<th>Finalise</th>
<th>Upload</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Engage stakeholders.</td>
<td>• Get relevant background information.</td>
<td>• Hold stakeholder discussion.</td>
<td>• Finalise RCA.</td>
<td>• Upload RCA in the tool.</td>
</tr>
<tr>
<td>• Understand business objectives or service level agreements.</td>
<td>• Identify key risks.</td>
<td>• Evaluate extreme risks.</td>
<td>• Agree on corrective actions for open risks.</td>
<td>• Enter controls in the control repository.</td>
</tr>
<tr>
<td>• Scope RCA.</td>
<td>• Prepopulate RCA template.</td>
<td>• Evaluate controls.</td>
<td>• Obtain approval for corrective actions and expected risks acceptance.</td>
<td>• Remove outdated legacy risks.</td>
</tr>
</tbody>
</table>

### Figure 3—Example RACI Chart

<table>
<thead>
<tr>
<th>Risk/Control/Actions</th>
<th>CEO</th>
<th>COO</th>
<th>Risk Officer</th>
<th>Head of Facilities</th>
<th>Chief of Security</th>
<th>Head of HR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Managing physical security</td>
<td>I</td>
<td>C, I</td>
<td>C, I</td>
<td>A</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>Reporting physical security incidents—employees and vendors</td>
<td>I</td>
<td>A</td>
<td>C, I</td>
<td>C, I</td>
<td>R</td>
<td>C, I</td>
</tr>
</tbody>
</table>
backgrounds and understanding of risks and controls and at various locations. The challenge was managed by creating additional training programs at various levels. This involved:

- Creating risk experts (typically with background experience and certifications such as Certified Information Systems Auditor™ [CISA®] and Chartered Accountant [CA]) across the regions and offices who were trained under a train-the-trainer program. Such resources were used to train the stakeholders.
- Tailoring the training delivered by the risk experts to the audience. For entity owners, a simple process overview was provided through mandatory computer-based training. For risk and control owners, training was detailed and included examples and tests, and it was delivered through classrooms at different locations or through web-based training sessions.
- Offering, as part of the mandatory training program, an awareness training session that explained the process and provided links and contacts for local risk experts within the organisation for further information and guidance.
- Arranging a workshop to disseminate the relevant information to stakeholders; this should begin any risk assessment process. The training resources were used to facilitate the control self-assessment (CSA) at different locations.
- Modifying the role description and performance evaluation process to include specific tasks for risks and controls.

**Benefit of Step 4**
Due to this top-down approach, the importance of risk management was well accepted and it was effective at all levels of the organisation.

**Step 5—Using a Reporting Tool**
A simple spreadsheet was used for maintaining a risk and control repository for each entity. Within the entity, the risk team member used an Excel spreadsheet for tracking risks, actions, etc. However, there was a requirement to have a single, common database repository for maintaining organisationwide risks and controls. Hence, a tool was developed to gather information for all entities. This helped in:

- Tracking all risks related to a 'service'
- Centralising a repository for all risks and control information
- Tracking all actions defined and agreed to in the RCA process
- Tracking closure of actions
- Reporting to senior executives on risks based on the specific requirements and levels of risk
- Basing regulatory requirements reporting on a common, single database of risks and controls.

**Benefit of Step 5**
A single repository of all risks, controls and actions was used by assurance teams in their reporting to the chief information officer (CIO) and for tracking compliance at a high level.

**Conclusion**
The entire development and implementation of the new process took almost two years. While the central team was responsible for developing the process, the location-based risk resources were instrumental in implementation, training, etc. Since the implementers at the different locations were part of the team, their feedback was used in making suitable changes and corrections that helped improve the maturity of the process.

Other tangible benefits of this initiative included:

- Prior to this implementation, there were more than 500 entities for which risks and controls were tracked. The number was optimised to around 100 entities. This was possible due to the implementation of the key entity management model.
- Earlier, there were more than 1,000 controls defined. The number was reduced as each control was mapped to the COBIT framework. At the global level, the number of controls was reduced to almost 350. However, within a particular entity, region, country, etc., further drilling down of a control was allowed for tracking locally. For example, globally, in the RCA, a single control was identified for local compliances: local regulatory compliance control. However, this control was further drilled down to various compliances based on country-specific requirements. In India, for example, this was managed through a separate spreadsheet that covered all of the Indian regulations, such as employee/labor laws and taxation regulations.
- The exercise helped the bank in managing risk and control process for Sarbanes-Oxley and other regulatory processes. The RCA spreadsheet provided a separate filter for Sarbanes-Oxley compliance applicability.
- The process repository in the tool helped in maintaining consistency. This was done by creating a separate sub-unit within the risk team to check the quality of each RCA before it was entered in the RCA tool.
A common training pack was seen as an important and valuable deliverable by the risk team and was defined based on the audience. For example, a training pack of 15 minutes for all entity owners (typically centre heads in each country or region) was developed and implemented using the e-learning portal, whereas a detailed process training pack was developed for risk and control owners.

Jitendra Barve, CISA, FCA
is a certified accountant with more than 18 years of experience in accounting, finance, audit and consulting. He has spent more than 10 years in information security audits and consulting and has worked on various assignments on risk management, risk-based internal audits, and information security reviews and audits. Barve is a board member of the ISACA Pune Chapter (India). He is associated with a mid-sized CA firm from Pune, G.D. Apte and Co.

Editor’s Note
Readers may wish to note that ISACA’s Risk IT framework expands on the areas covered in this article and supports enterprises in identifying, governing and managing IT-related business risks, complementing the control (risk mitigation) guidance provided in COBIT. Click here for more information on Risk IT.

Laugh & Learn: Using COBIT to Improve the Software Development Life Cycle
By Corjan Bast

Improving IT governance or implementing COBIT can seem very easy on paper, but the actual exercise usually is not. Part of the difficulty is that many people do not understand the COBIT concepts or, when they do, they find it difficult to explain to someone what COBIT provides. Fortunately, humor can help a great deal in helping someone “understand.” The anecdotal example included here builds on this to explain how COBIT can be used to improve the software development life cycle, one of the many aspects in which COBIT can be used to enhance IT governance.

Anecdotal Example
1. Programmer produces code that is believed to be bug-free.
2. Product is tested. Twenty-six bugs are found.
3. Programmer fixes 16 of the bugs and explains to the testing department that the other 10 are not really bugs.
4. Testing department finds that five of the fixes did not work and discovers 14 new bugs.
5. Repeat step 3.
7. Due to pressure from the business and an extremely premature product announcement based on an overly optimistic programming schedule, the product is released.
8. Users find 139 new bugs.
9. Original programmer is no longer with the company.
10. Newly assembled programming team fixes almost all of the 139 bugs, but introduces 567 new ones.
11. Original programmer sends underpaid and overworked testing department a postcard from Hawaii. Entire testing department quits.
12. Company is bought in a hostile takeover by competitor using profits from its latest release, which had 687 bugs.
13. New CEO is brought in by board of directors. He hires a programmer to redo program from scratch.
14. Programmer produces code that is believed to be bug-free…

Learning Point
Obviously something goes wrong during the software development life cycle, but unfortunately, nothing is changed for the better. Although the situation in the example is, of course, a bit exaggerated, the nature of the example is applicable to many organizations: Things go wrong and will go wrong, but finding the correct improvements and driving the change is another story.

COBIT can be used to improve the situation in the example. COBIT’s Acquire and Implement (AI) domain provides guidance so that the business objectives/goals linked to the software development projects will be successfully met. The COBIT AI5
**Procure IT resources** process, for example, will help ensure that the correct IT skills are available, while **AI7 Install and accredit solutions and changes** minimizes errors creeping into live production due to incomplete testing. In turn, these COBIT processes can be supported by IT Infrastructure Library (ITIL) processes, such as release management, deployment management and change management, for greater detail.

According to COBIT, executives and the board of directors are ultimately responsible for the governance of IT. It is essential that they provide leadership, organizational structures and processes to enable IT to deliver value and support the organization’s strategies and objectives. This is clearly not the case in the example.

To help organizations implement COBIT and be able to change the organization, ISACA released the guide *Implementing and Continuously Improving IT Governance* in late 2009. The guide not only focuses on implementing COBIT, but it also talks a great deal about enabling a change in culture, which is necessary throughout any implementation. Perhaps after reading the implementation guide, changing the organization to use COBIT will not be too hard after all.

**Corjan Bast**
is global product manager of ITpreneurs, where he is responsible for overseeing the IT governance portfolio. He works closely with experts at standards authorities to shape best practice standards into innovative learning solutions. In addition, he collaborates with other professionals to publish articles and present the latest trends in the IT governance arena at industry consortia events. Previously, Bast was an IT governance consultant for a firm that focused on assisting Fortune 1,000 organizations implementing IT governance frameworks, such as COBIT and Val IT. He currently resides in Tampa, Florida, USA, and can be reached at corjan.bast@itpreneurs.com.

**Using COBIT and COSO ERM**

**By Christopher Fox, ACA**

While ISACA offers numerous mappings of various standards and guidance documents to COBIT that are subsets of the COBIT framework, no mapping has been undertaken between COBIT and the Committee of the Sponsoring Organizations of the Treadway Commission’s *Enterprise Risk Management—Integrated Framework* (COSO ERM). In this case, COBIT is the subset.

However, given the importance of each of these documents and the widespread use of both frameworks within enterprises worldwide, this article presents a proposed mapping between the two. Its purpose is to provide assistance to those charged with aligning IT efforts with the overall corporate enterprise risk framework (represented by COSO ERM).

**Methodology for the Mapping**
The COSO ERM framework does not specifically address information management and IT. However, IT is an implied part of any system of internal controls, regardless of the type of risk (financial statements, regulatory or operational), and, consequently, forms an important element in organizationwide risk management. The COBIT framework offers a defined and recognized set of IT control processes, objectives and activities designed to adapt IT risk management to the requirements of COSO ERM and regulatory drivers. COBIT, therefore, bridges the gap between high-level enterprise risk management (ERM) and specific IT risk issues.

As noted, unlike the mappings in ISACA’s *COBIT Mapping Series*, in which a detailed framework represents a subset of the COBIT framework, COBIT represents a subset of the COSO ERM framework (see **figure 1**). However, an organization should have an IT risk management competency in all COSO ERM components.

The mapping of COBIT to COSO ERM described in this article was a subjective exercise. To reduce the subjectivity of the
**Components of ERM:**
- **Internal environment**—The entity’s internal environment is the foundation for all other components of ERM, providing discipline and structure.
- **Objective setting**—Within the context of the established mission or vision, management establishes strategic objectives, selects strategy and establishes related objectives.
- **Event identification**—As part of event identification, management considers external and internal factors that affect event occurrence.
- **Risk assessment**—Risk assessment allows an entity to consider how potential events may affect the achievement of objectives.
- **Risk response**—Management identifies risk response options and considers their effect on event likelihood and impact.
- **Control activities**—Control activities are the policies and procedures that help ensure that risk responses are properly executed.
- **Information and communication**—Pertinent information from internal and external sources must be identified, captured and communicated in a form and time frame that enable personnel to carry out their responsibilities.
- **Monitoring**—ERM is monitored using a process that assesses both the presence and functioning of its components and the quality of their performance over time.

**The Mapping**
Professional judgment was then used to assess the extent of fit that a COBIT control process has with the COSO ERM objectives and components, resulting in the mapping illustrated in figure 2. The second column, IT Governance Focus Area, represents the five areas of IT governance, as defined by ISACA.
Figure 2—Mapping of COBIT and COSO ERM

<table>
<thead>
<tr>
<th>COSO ERM Objectives and Components</th>
<th>IT Governance Focus Area</th>
<th>Contribution of COBIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strategic Alignment</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Value Delivery</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Resource Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance Measurement</td>
<td></td>
</tr>
<tr>
<td>Objectives</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Strategic**

+ + + + +

Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM objective are:

- PO1 Define a strategic IT plan
- PO3 Determine technological direction
- PO4 Define the IT processes, organization and relationships
- PO6 Communicate management aims and direction
- ME1 Monitor and evaluate IT performance
- ME4 Provide IT governance

**Operations**

+ + + + +

Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM objective are:

- PO5 Manage the IT investment
- PO8 Manage quality
- ME1 Monitor and evaluate IT performance
- ME2 Monitor and evaluate internal control
- ME4 Provide IT governance

**Reporting**

+ + + + +

Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM objective are:

- PO6 Communicate management aims and direction
- PO8 Manage quality
- DS6 Identify and allocate costs

**Compliance**

+ + + + +

Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM objective are:

- PO4 Define the IT processes, organization and relationships
- PO6 Communicate management aims and direction
- PO9 Assess and manage IT risks
- DS2 Manage third-party services
- DS4 Ensure continuous service
- DS5 Ensure systems security
- DS7 Educate and train users
- ME2 Monitor and evaluate internal control
<table>
<thead>
<tr>
<th>COSO ERM Objectives and Components</th>
<th>IT Governance Focus Area</th>
<th>Contribution of COBIT</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Strategic Alignment</td>
<td></td>
</tr>
<tr>
<td>Internal environment</td>
<td>Value Delivery</td>
<td>• ME3 Ensure compliance with external requirements</td>
</tr>
<tr>
<td></td>
<td>Resource Management</td>
<td>• ME4 Provide IT governance</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Performance Measurement</td>
<td></td>
</tr>
<tr>
<td>Objective setting</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event identification</td>
<td>+ + + +</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+ + + +</td>
<td></td>
</tr>
</tbody>
</table>

Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:
- PO4 Define the IT processes, organization and relationships
- AI4 Enable operation and use
- DS4 Ensure continuous service
- DS7 Educate and train users
- ME2 Monitor and evaluate internal control
- ME3 Ensure compliance with external requirements
- ME4 Provide IT governance

- PO1 Define a strategic IT plan
- PO5 Manage the IT investment
- PO6 Communicate management aims and direction
- DS1 Define and manage service levels
- DS3 Manage performance and capacity
- DS4 Ensure continuous service
- DS5 Ensure systems security
- DS7 Educate and train users
- ME1 Monitor and evaluate IT performance

- PO6 Communicate management aims and direction
- PO9 Assess and manage IT risks
- PO10 Manage projects
- DS2 Manage third-party services
- DS4 Ensure continuous service
- DS5 Ensure systems security
- DS8 Manage service desk and incidents
- DS10 Manage problems
## COSO ERM Objectives and Components

<table>
<thead>
<tr>
<th>IT Governance Focus Area</th>
<th>Strategic Alignment</th>
<th>Value Delivery</th>
<th>Risk Management</th>
<th>Resource Management</th>
<th>Risk Management</th>
<th>Performance Measurement</th>
</tr>
</thead>
</table>

### Risk assessment

- Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:
  - PO6 Communicate management aims and direction
  - PO9 Assess and manage IT risks
  - PO10 Manage projects
  - DS2 Manage third-party services
  - DS4 Ensure continuous service
  - DS5 Ensure systems security
  - DS8 Manage service desk and incidents
  - DS10 Manage problems
  - ME4 Provide IT governance

### Risk response

- Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:
  - PO6 Communicate management aims and direction
  - PO9 Assess and manage IT risks
  - PO10 Manage projects
  - DS2 Manage third-party services
  - DS4 Ensure continuous service
  - DS5 Ensure systems security
  - DS8 Manage service desk and incidents
  - DS10 Manage problems
  - ME1 Monitor and evaluate IT performance

### Control activities

- Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:
  - AI1 Identify automated solutions
  - AI2 Acquire and maintain application software
  - AI7 Install and accredit solutions and changes
  - DS1 Define and manage service levels
  - DS4 Ensure continuous service
  - DS5 Ensure systems security
  - DS8 Manage service desk and incidents
  - DS9 Manage the configuration
  - DS10 Manage problems
  - DS11 Manage data
<table>
<thead>
<tr>
<th>COSO ERM Objectives and Components</th>
<th>IT Governance Focus Area</th>
<th>Contribution of COBIT</th>
</tr>
</thead>
</table>
| Information and communication     | + + + + +                | DS12 Manage the physical environment  
                                 |                          | DS13 Manage operations |
| Monitoring                        | + + + + +                | Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:  
                                 |                          | PO5 Manage the IT investment  
                                 |                          | AI1 Identify automated solutions  
                                 |                          | AI7 Install and accredit solutions and changes  
                                 |                          | DS1 Define and manage service levels  
                                 |                          | DS3 Manage performance and capacity  
                                 |                          | DS4 Ensure continuous service  
                                 |                          | DS5 Ensure systems security  
                                 |                          | DS6 Identify and allocate costs  
                                 |                          | DS8 Manage service desk and incidents  
                                 |                          | DS10 Manage problems  
                                 |                          | ME4 Provide IT governance |
|                                  |                          | Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this COSO ERM component are:  
                                 |                          | PO4 Define the IT processes, organization and relationships  
                                 |                          | PO9 Assess and manage IT risks  
                                 |                          | PO10 Manage projects  
                                 |                          | 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  
                                 |                          | DS8 Manage service desk and incidents  
                                 |                          | DS10 Manage problems  
                                 |                          | ME1 Monitor and evaluate IT performance  
                                 |                          | ME2 Monitor and evaluate internal control  
                                 |                          | ME3 Ensure compliance with external requirements  
                                 |                          | ME4 Provide IT governance |
Conclusion
By mapping COBIT and COSO ERM, professionals can:

- Assess how enterprise-level control and process frameworks map to a specific IT governance framework
- Assist in aligning IT efforts with the overall corporate enterprise risk framework
- Assist in identifying gaps that may not be addressed by detailed frameworks

Threats to IT can be catastrophic. Organizations will greatly benefit by the thorough risk management that will be in place when using COBIT and COSO ERM together.

Editor's Note
Those enterprises looking to combine COBIT and risk management, to achieve the benefits referred to in the conclusion of this article, should also consider using the Risk IT framework and supporting materials from ISACA®. The Risk IT Framework helps enterprises to bridge the gap effectively between generic risk management frameworks, such as COSO ERM, and more detailed IT risk management and control frameworks, including COBIT. Click here for more information on Risk IT.

Christopher Fox, ACA
was, until recently, a senior operational and technology risk and compliance executive. He has proven ability to facilitate profitability and operational success through global risk and compliance management. Fox has significant experience in addressing Basel II, the US Sarbanes-Oxley Act, and other global regulatory and industry requirements. He is a subject matter expert on COSO, COBIT, Sarbanes-Oxley, risk and compliance, information security, and regulatory support, among other areas. Fox is experienced at leading global audits and regulatory mediation projects in Europe, Indonesia, Malaysia, Thailand, the US and other countries.
Mapping FFIEC Framework With COBIT 4.1

By Kenny Lee, CISA, CISM, CISSP

When people read articles or job postings related to governance of IT, risk management, security or audit, they will often see the typical alphabet soup: ITIL, NIST, FFIEC, ISO 27002 (17799) and COBIT. ISACA and its volunteers have made significant efforts to map many of these standards and frameworks to COBIT. These mappings and COBIT provide ISACA members and constituents a proven governance of IT framework that can be leveraged in their organizations along with other applicable frameworks and standards.

Mapping the US Federal Financial Institutions Examination Council (FFIEC) Information Technology Examination Handbook (IT Handbook) to COBIT has been a long time coming. The ISACA Los Angeles (California, USA) Chapter knew that mapping the FFIEC IT Handbook to COBIT would be valuable to ISACA members because of the heightened financial regulatory scrutiny of financial institutions. The mapping research and expert review team included associates of major accounting firms, financial institutions and the US Federal Deposit Insurance Corporation (FDIC).

It is hoped that this latest mapping publication, COBIT® Mapping: Mapping FFIEC Framework With COBIT® 4.1, will be a valuable addition to ISACA’s growing COBIT mapping library and that it will be continually revised as the FFIEC IT Handbook and COBIT are updated in the future.

We Know COBIT…What Is FFIEC?
Here is a description of FFIEC from its web site:

The Federal Financial Institutions Examination Council is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Office of Thrift Supervision (OTS), and to make recommendations to promote uniformity in the supervision of financial institutions. In 2006, the State Liaison Committee (SLC) was added to the Council as a voting member. The SLC includes representatives from the Conference of State Bank Supervisors (CSBS), the American Council of State Savings Supervisors (ACSSS), and the National Association of State Credit Union Supervisors (NASCUS).

The FFIEC IT Handbook now makes the expectations of IT examiners easier to understand and easier with which to comply. Although the booklets that make up the FFIEC IT Handbook are intended for a wide-ranging audience, the content is written at a level appropriate for a midlevel IT examiner. There are 11 booklets, each focusing on a topic that offers general control and audit guidance:

- Audit
- Business Continuity Planning
- Development and Acquisition
- E-banking*
- Information Security
- Management
- Operations

Click here to visit the ISACA Bookstore to order.
Outsourcing Technology Services
Retail Payment Systems*
Supervision of Technology Service Providers*
Wholesale Payment Systems*

It is important to note that only seven of the FFIEC IT Handbook booklets were mapped to COBIT for the ISACA mapping. The four booklets marked with asterisks in the previous list were found to be too narrow in scope for the mapping.

Readers should also know that the FFIEC included “work programs” (audit checklists) that nicely complement the booklets. While the work programs were not mapped to COBIT in COBIT Mapping: Mapping FFIEC Framework With COBIT 4.1, it is worthwhile for both examiners and auditors, as well as those who wish to understand an examiner’s objectives and procedures, to look over these documents.

**How to Get Started/What to Expect**

To facilitate the mapping process between the FFIEC IT Handbook and COBIT 4.1, a custom index was developed for the booklets to provide feasible reference points. The custom FFIEC IT Handbook index is located in the appendix of the document.

Mapping details between the FFIEC booklets and COBIT have been documented in Microsoft Word format and can be difficult to read. Therefore, the project team also included the mapping in a Microsoft Excel format for ease of use (e.g., to allow for filtering and sorting).

When reading, referencing and digesting the document, there are a few important points that should be kept in mind:

- COBIT should be used as the umbrella framework, not as a standard or regulatory requirement framework. COBIT is a governance of IT framework to which other specific standards, regulatory requirements and IT frameworks can be mapped to provide a broad governance of IT context; however, it should not be used as a substitute for any regulatory requirements that are applicable to financial institutions.
- The FFIEC IT Handbook is the guidance (not COBIT) that is used for the federal examination of financial institutions by the FRB, FDIC, NCUA, OCC and OTS and that is used to make recommendations to promote uniformity in the supervision of financial institutions.
- The mapping of the FFIEC IT Handbook and COBIT framework provides value to financial institutions that have already adopted the COBIT framework for governance of IT, for compliance with section 404 of the US Sarbanes-Oxley Act, or as a risk and control framework. As mentioned previously, since COBIT does not cover the specific details necessary to be in compliance with FFIEC requirements, the COBIT to FFIEC mapping can be used as a reference guide to dive into the details of the FFIEC IT Handbook, using the COBIT framework that is familiar to the organization.

As is true with any IT project, it is important to ensure that all appropriate parties be involved with the activities related to the FFIEC IT Handbook and COBIT (e.g., adoption/implementation, control assessment, examination/audit). COBIT’s Responsible, Accountable, Consulted and Informed (RACI) charts and the roles and responsibilities sections within the FFIEC IT Handbook booklets can provide guidance on the parties involved. Communication is key.

**COBIT Mapping: Mapping FFIEC With COBIT 4.1** is now available on the ISACA web site as a free download to ISACA members and for purchase to nonmembers. Click here for more information on ISACA research projects.

**Author’s Note**

Please remember that this document is the result of countless volunteer hours contributed by ISACA Los Angeles Chapter volunteers. In the spirit of volunteerism, readers are encouraged to also volunteer and get involved with ISACA and local chapters. Without volunteers, publications such as this would not be possible. Click here to learn more.

**Kenny Lee, CISA, CISM, CISSP**

is a vice president of technology operational risk management at Bank of America. He previously served as ISACA Los Angeles Chapter’s vice president and director of COBIT. He currently resides in Seattle, Washington, USA. His areas of expertise include enterprise resource planning controls and security, network and application security, technology risk management, and IS audit.

**Endnote**

1 US Federal Financial Institutions Examination Council (FFIEC), www.ffiec.gov
New COBIT Case Study: Ecopetrol S.A.

Ecopetrol S.A. is a vertically integrated crude oil and natural gas company engaged in the exploration, development and production of crude oil and natural gas. In 2007, Ecopetrol updated its corporate strategy with clearly defined growth goals for the next years that required important changes and improvements in the organizational structure and processes that support the strategic objectives.

Consequently, there were important milestones, such as the transformation of the legal nature of the company, the initiation of international operations and the adoption of the COSO framework to strengthen the internal control system. The company listed its shares on the New York Stock Exchange in September 2008. Aligned with the strategic deployment and to provide timely and effective response to the requirements generated by the company's situation, the Information Technology Division decided in 2008 to integrate an IT management system, based on a proper framework. COBIT was selected as the appropriate governance of IT framework to implement its IT management system.

Ecopetrol plans to finish 2010 with 31 COBIT processes built into the IT management system, operating at level 3, with a view to achieve level 4 in 2011. The Information Technology Division is studying the draft documents of COBIT 5 and plans to implement it as soon as it is available. Ecopetrol is also extending the practices of its IT management system and COBIT to the companies in its business group in Colombia, Peru and Brazil. The IT management system will be embedded in the corporate management system to ensure integration and alignment of practices.

Click here for the full text of this and other COBIT case studies.