WHAT'S NEW IN COBIT 4.0
George H Bodnar
Internal Auditing; Jul/Aug 2006; 21, 4; ABI/INFORM Global pg. 37

WHAT’S NEW IN COBIT 4.0

The latest edition of this IT control framework will help organizations get a handle on IT governance and Sarbanes-Oxley compliance.

COBIT 4.0

Managment must satisfy quality, fiduciary, and security requirements for the organization’s information assets as it must for all of the organization's assets. Management should also optimize the use of an organization’s available resources, including information technology (IT) resources, and must understand the status of an organization’s IT systems and determine the levels of security and control that these systems should provide.

COBIT 4.0 is a publication that is directed at helping management discharge its responsibilities with respect to an organization’s IT assets by “bridging the gaps” between business risks, control needs, and technical issues. COBIT provides “good practices” across a domain and process framework and presents activities in a manageable and logical structure. COBIT’s term “good practices” means that these practices represent a consensus of IT experts. These practices will help management optimize the organization’s information investments and will provide measures that may serve as benchmarks to be judged against when activities and events do not go according to plan.

COBIT development and IT governance
COBIT is an acrronym for Control Objectives for Information and related Technology. It is an open standard for control over IT, available for free download online at www.isaca.org/cobit.

COBIT identifies 34 IT processes, a high-level approach to control over these processes, and 318 detailed control objectives and audit guidelines to assess the IT processes. It provides a generally applicable and accepted standard for IT security and control practices and is designed to guide and assist management in determining and monitoring the appropriate level of IT security and control for an organization.

“IT governance” is an inclusive term that encompasses the variety of elements that interact to provide IT services within an organization. These elements include communication, business, legal, and other issues, as well as management, IT users, IT staff, suppliers, auditors, and other parties. IT governance has the objective of enhancing and ensuring the efficient application of IT resources as a critical success factor.

The IT Governance Institute is the publisher of COBIT 4.0, and was the primary publisher of COBIT 3rd Edition in July 2000. The third edition expanded the work that was initially published by the Information Systems Audit and Control Foundation (ISACF) in 1996. The second edition was published two years later in 1998. Also in 1998, the Information Systems Audit and Control Association (ISACA) and the ISACF created the IT Governance Institute for the purpose of advancing the understanding and adoption of IT governance principles.

COBIT 3rd Edition reflected the influence of the IT Governance Institute through the addition of a management guidelines...
component and its expanded and enhanced focus on IT governance. The management guidelines were comprised of:
- maturity models, which provided for strategic choice and benchmark comparison;
- critical success factors, which provided for getting IT processes under control;
- key goal indicators, which provided for monitoring achievement of IT process goals; and
- key performance indicators, which provided for monitoring performance within each of CobiT’s 34 IT processes.

CobiT 4.0 continues and enhances this work. ISACA’s control objectives served as the foundation of the first edition of CobiT. CobiT has subsequently been expanded and enhanced through the assimilation of current and emerging international technical, professional, regulatory, and industry-specific standards. The resulting control objectives are applicable to organization-wide information systems. With respect to IT, the phrase “generally applicable and accepted” is explicitly used in CobiT to have the same type of meaning as the phrase generally accepted accounting principles (GAAP) in the financial environment.

CobiT is designed to be used by management, IT users, and auditors. Management can use CobiT to assist in balancing risk and control investment in the often unpredictable IT environment. Users of IT can use CobiT to obtain assurance concerning the security and associated controls of IT services that are provided by internal or third parties. Auditors can use CobiT to substantiate their opinions and/or provide advice to management on internal controls.

Cross-references between CobiT 3rd Edition and CobiT 4.0

Development of the CobiT framework content is supervised by the CobiT Steering Committee, which consists of international representatives from industry, academia, government, and the IT governance, assurance, control, and security professions. International working groups have been established for the purpose of quality assurance and expert review of the project’s interim research and development deliverables. Overall project guidance is provided by the IT Governance Institute.

The update to the control objectives in CobiT 3rd Edition, based on new and revised international references, was conducted by members of ISACA chapters, under the guidance of the CobiT Steering Committee members. The intention was not to perform a global analysis of all material or a redevelopment of the control objectives, but to provide an incremental update process. The results of the development of the management guidelines were then used to revise the framework, especially the considerations, goals, and enable statements of the high-level control objectives.

Appendix V of CobiT 4.0 provides cross-references between CobiT 3rd Edition and CobiT 4.0 in three categories: framework-level changes, detailed control objectives, and management guidelines.

The major changes to the CobiT framework as a result of the CobiT 4.0 update are as follows:
- The M domain has now become ME, standing for Monitor and Evaluate.
- M3 and M4 in CobiT 3rd Edition have been removed, as they were audit processes.
- ME3 is now the process related to regulatory oversight, which was previously covered by P08.
- ME4 now covers the process of governance oversight over IT.
- P08 now becomes Manage Quality, the old PO11 process. The PO domain now has 10 processes instead of 11.
- A15 is now the procurement process. Old A15 has become A17. The A1 domain now has seven instead of six processes.

Despite these changes to the framework, there remain 34 control objectives.

Comparison of presentation format: CobiT 4.0 vs. CobiT 3rd Edition

There is a significant structural difference in the overall presentation format of CobiT 4.0 versus CobiT 3rd Edition.

In CobiT 3rd Edition, the framework, management guidelines, and control objectives were each published as a separate
book. Each control objective was separately presented in each of these different books, in a format appropriate to the context. As a printed document, each management guideline was two pages. On the left-hand page, every management guideline provided a process identification statement, a goal statement, and others items, including critical success factors, key goal indicators, and key performance indicators. A maturity model was provided on the right-hand page of each guideline. The framework book had a single page for each control objective. This page illustrated a "waterfall" diagram for each control objective. The control objectives book presented detailed descriptions for each of the high-level control objectives. The control objectives book also contained the "waterfall" diagram for each high-level control objective that was in the separate framework book.

CobiT 4.0 is a single document rather than a collection of separate books. Thus, the overall presentation is integrated. The equivalent elements are grouped together and presented only once for each control objective. In CobiT 4.0, each high-level control objective is presented with the following collection of items:

• CobiT navigation diagram: This is an updated version of the "waterfall" diagrams that were presented for each control objective in CobiT 3rd Edition.
• Detailed control objectives: These are similar and the equivalent of those contained in a separate book in CobiT 3rd Edition.
• Management guidelines: These are presented as charts and figures, rather than narrative text.
• Maturity model: These are very similar and the equivalent of those contained in the separate management guidelines book in CobiT 3rd Edition. Each of these elements is compared and contrasted between 4.0 and the 3rd Edition.

Framework navigation

**CobiT 4.0 navigation diagram.** For each of the CobiT IT processes, a high-level control objective statement is provided, together with key goals and metrics in the form of a waterfall diagram. Each framework step is successively indented to give the diagram a waterfall-like appearance, as shown in Exhibit 1.

In addition, each of the corners in the diagram contains a graphic that provides additional context:
• In the upper left corner, a 3-D bar chart of information criteria is shown with the following labels in individual bars: Effectiveness, Efficiency, Confidentiality, Integrity, Availability, Compliance, and Reliability. In each diagram, one of these criteria is indicated as primary and another as secondary by including P or S on the bar that contains the criteria.
• In the upper right corner, the four CobiT domains are shown in button-like graphics: Plan and Organize, Acquire and Implement, Deliver and Support, and Monitor and Evaluate. The relevant domain is indicated with an enlarged button.
• In the lower left corner, a pentangle figure of IT governance focus areas is

---

**EXHIBIT 1** CobiT Navigation Waterfall Diagrams

CobiT 4.0 Waterfall Diagram

Control over the IT process of process name

that satisfies the business requirement for IT of summary of most important business goals

by focusing on summary of most important IT goals

is achieved by key controls

and is measured by key metrics

CobiT 3rd Edition Waterfall Diagram

The control of IT processes

which satisfy business requirements

is enabled by control statements

considering control practices

---

Reproduced with permission of the copyright owner. Further reproduction prohibited without permission.
shown with the following labels in individual segments: Strategic Alignment, Performance Measurement, Value Delivery, Risk Management, and Resource Management. One of these focus areas is indicated as primary and another as secondary by shading the appropriate segment P (dark) or S (gray).

- In the lower right corner, a 3-D bar chart of IT resources appears with the following labels in individual bars: Applications, Information, Infrastructure, and People. Checkmarks indicate resources that are of concern to the process.

Comparison to CobiT 3rd Edition navigation diagram. The navigation diagram as it appeared in the 3rd Edition is also shown in Exhibit 1. The obvious difference is that there are four rather than five steps. The second step, "which satisfy business requirements," has been expanded to two steps in CobiT 4.0, "that satisfies the business requirement for IT off/summary of most important business goals" and "by focusing on/summary of most important IT goals." The third and fourth steps, "is enabled by/control statements" and "considering/control practices," is changed in CobiT 4.0 to "is achieved by/key controls" and "and is measured by/key metrics." The change of the last step highlights the fact that one of the major changes has been the effort to make metrics more representative and measurable.

Only three of the corners in the 3rd Edition contained a graphic—the lower left corner was empty. Thus, the pentangle figure of IT governance focus areas is new in CobiT 4.0. Also, in the lower right corner, the 3-D bar chart of IT resources listed five resources: People, Applications, Technology, Facilities, and Data. The change to four resources in CobiT 4.0 means that Information and Infrastructure replace Technology, Facilities, and Data.

Detailed control objectives
The updating of the CobiT framework has significantly changed the detailed control objectives within it. These components have been reduced by almost one third, from 318 to 215. This reduction occurs as all generic materials are now retained only at the framework level and are not repeated in each process. Also, all references to applications controls were moved to the framework and specific control objectives were aggregated into new statements. In order to support transitional activity in relation to control objectives, Appendix V of CobiT 4.0 contains two detailed tables that provide cross-references between the two sets of detailed control objectives.

Management guidelines
The presentation of management guidelines has both changed and expanded in CobiT 4.0. The management guidelines component was first included in the 3rd Edition and demonstrated the expanded and enhanced focus on IT governance. The guidelines were the result of research conducted by industry experts, analysts, and academics from around the world. They addressed management's need for control and measurability of IT by providing tools to assess and measure an organization's IT environment against the 34 IT processes identified by CobiT.

Overall risk management and assurance are dependent on specific management practices. In order to successfully discharge its obligations, management requires condensed and up-to-date information that enables it to make difficult decisions on risk and control in a timely fashion. Conceptually, this process is likened to the use of dashboards to "keep the ship on course," scorecards to achieve results that are satisfactory for the largest possible group of stakeholders, and benchmarking to enable the organization to adapt to trends and developments in the environment. Dashboards are constructed with indicators, scorecards record measurements, and benchmarking implies and thus requires some type of measurement scale to enable comparison.

As first issued in the 3rd Edition, the management guidelines were comprised of maturity models, critical success factors, key goal indicators, and key performance indicators. Maturity models provided for strategic choice and benchmark comparison. Critical success factors provided for getting IT processes under control. Key goal indicators provided for monitoring
achievement of IT process goals. Finally, Key performance indicators provided for monitoring performance within each of CobiT's 34 IT processes.

As CobiT 4.0 is the first revision to CobiT since the original issuance of the management guidelines, it is not surprising that these have been significantly modified. Stated changes are summarized as follows:

- Inputs and outputs have been added to illustrate what processes require from other processes and what the processes typically deliver.
- Activities and associated responsibilities have also been provided.
- Inputs and activity goals replace the critical success factors of CobiT 3rd Edition.
- Metrics are now based on a consistent cascade of business goals, IT goals, process goals, and activity goals.
- The CobiT 3rd Edition metrics set has also been reviewed and enhanced to make it more representative and measureable.

It is noted that while this material is collected from hundreds of experts, following rigorous research and review, the inputs, outputs, responsibilities, metrics, and goals are illustrative but not prescriptive or exhaustive. They provide a basis of expert knowledge from which each enterprise should select what efficiently and effectively applies to it based on enterprise strategy, goals, and policies.

**Inputs, outputs, and activities.** Inputs, outputs, and activities collectively replace the critical success factors of CobiT 3rd Edition. Critical success factors provided for getting IT processes under control. They consisted of important activities that contribute to the IT process achieving its goals, and could be strategic, technical, organizational, process, or procedural in nature. The "critical success factors" concept in CobiT 3rd Edition was likened to a standard feedback control system in which one sets room temperature (the standard) and the heating system (process) constantly checks (compares) temperature (the control information) and will signal (act) the heating system to provide more heat. The following were examples of critical success factors that usually would apply to any process: defined and documented processes, defined and documented policies, clear accountabilities, and consistent measurement practices.

In CobiT 4.0, the process inputs indicate what the process owner needs from other processes. Inputs are presented in a two-column table indicating the source of the input and the input in question. As an illustration, the first two of the eight inputs for process PO1, Define a Strategic IT Plan, are cost/benefits reports and risk assessment.

The process outputs are what the process owner has to deliver. This is also presented as a table. The first column indicates the output, while subsequent columns may vary in number and indicate the destination of the output. As an illustration, the first two of the six outputs for process PO1 are strategic IT plan and tactical IT plan.

Documentation and assignment of activities in a RACI chart is a new feature in CobiT 4.0. A RACI chart identifies who is Responsible, Accountable, Consulted, and/or Informed. Activities are listed in the first column of the chart, while subsequent columns identify functions that receive assignments. The roles in the RACI chart include the CEO, CFO, executives, the CIO, and business process owners, among others, including compliance, audit, risk, and security—functions with control responsibilities but which do not have operational IT responsibilities. For example, the first activity in the RACI chart for process PO1 is "Link business goals to IT goals," which is assigned as follows: CEO—C (consulted); CFO—I (informed); business executive—A/R (accountable/responsible); CIO—R (responsible); and business process owner—C (consulted).

**Goals and metrics.** Goals and metrics show how the process should be measured. The presentation of this material in CobiT 4.0 has been restructured to emphasize goals within each process. Activity goals are measured by key performance indicators (KPIs). Process and IT goals are measured by key goal indicators (KGI). CobiT 3rd Edition emphasized the metrics within each process; critical success factors, KPIs, and KGI were each presented as separate tables and goals were not explicitly specified.

KPIs are measures that indicate that a process is achieving its business requirements by monitoring the performance of the enablers of the process. They are lead indi-
icators of whether or not a goal will likely be reached. KPIs are process-oriented and often express how well resources are utilized. They are usually expressed as a number or percentage. A “good” KPI will accurately predict success or failure of attaining a process goal. KPIs are concerned with “how,” and should have a cause-and-effect relationship with the KGI of an activity. As an illustration, the following are the KPIs shown for the activity goals for process PO1:

- delay between updates of business strategic/tactical plan and updates of IT strategic/tactical plan;
- percentage of strategic/tactical IT plan meetings where business representatives have actively participated;
- delay between updates of IT strategic plan and updates of IT tactical plans;
- percentage of tactical IT plans complying with the predefined structure/contents of those plans; and
- percentage of IT initiatives/projects championed by business owners.

KGI s are representations of the goals of an IT process—they are targets to be achieved and measurable indicators of the process achieving its goals. KGI s are lag indicators, as they can only be measured after the fact. They are usually expressed in positive terms but may be expressed negatively, i.e., in terms of the impact of not attaining a goal. They should be explicit and measurable as a number or percentage. Management should set specific targets that need to be met, taking into account the past performance and future goals of an IT process. As an illustration, the following are the KGI s shown for the process PO1:

**Process KGI s:**

- percentage of IT objectives in the IT strategic plan that support the strategic business plan;
- percentage of IT initiatives in the IT tactical plan that support the tactical business plan; and
- percentage of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plan.

**IT KGI s:**

- degree of approval of business owners of the IT strategic/tactical plans;
- degree of compliance with business and governance requirements; and
- level of satisfaction of the business with the current state (number, scope, etc.) of the project and applications portfolio.

**Maturity models**

In CobiT 4.0, the maturity model component is the capstone of the management guidelines presentation. It is used to evaluate an organization’s relative level of achievement of IT governance. The defined levels in the scale are numbered 0 to 5, ranging from nonexistent (0) to optimized (5). The overall structure of this important component is the same as it was in CobiT 3rd Edition.

The maturity model shows what has to be done to improve. Risk and controls in IT management processes are inherently subjective and imprecise topics that are not amenable to the more mechanistic approach that is found in the maturity models for software engineering. Scales need to be practical to apply and reasonably easy to understand. The advantage of a maturity model approach is that it is relatively easy for members of management to place themselves on the scale and appreciate what is involved if they need to improve performance. The 0–5 scale indicates how a process evolves from nonexistent to optimized. The scale includes 0 because it is quite possible that no process exists at all.

CobiT 4.0 provides generic, qualitative descriptions of the six levels (0 to 5) in its maturity model. (See Exhibit 2.) The generic model is identical to the model in CobiT 3rd Edition. An organization might use a similar but different maturity model. CobiT suggests that whatever model an organization decides to use, the scales should not be too granular. Too many levels would make the model difficult to use and, more important, suggest a precision that is not justifiable. Rather, management should concentrate on maturity levels based on a set of conditions that can be met unambiguously.

The maturity model offers a way of measuring how well developed management processes are and how well developed they should be. Management can map each of CobiT’s 34 processes to the levels defined in the maturity model to determine:

- the organization’s current status—where it is today;
EXHIBIT 2 CobiT’s Generic Maturity Model for IT Processes

0 Non-Existent.
Complete lack of any recognizable processes. The organization has not even recognized that there is an issue to be addressed.

1 Initial.
There is evidence that the organization has recognized that the issues exist and need to be addressed. There are, however, no standardized processes; instead there are ad hoc approaches that tend to be applied on an individual or case-by-case basis. The overall approach to management is disorganized.

2 Repeatable.
Processes have developed to the stage where similar procedures are followed by different people undertaking the same task. There is no formal training or communication of standard procedures, and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely.

3 Defined.
Procedures have been standardized and documented, and communicated through training. It is, however, left to the individual to follow these processes, and it is unlikely that deviations will be detected. The procedures themselves are not sophisticated but are the formalization of existing practices.

4 Managed.
It is possible to monitor and measure compliance with procedures and to take action where processes appear not to be working effectively. Processes are under constant improvement and provide good practice. Automation and tools are used in a limited or fragmented way.

5 Optimized.
Processes have been refined to a level of best practice, based on the results of continuous improvement and maturity modeling with other enterprises. IT is used in an integrated way to automate the workflow, providing tools to improve quality and effectiveness, making the enterprise quick to adapt.

- the current status of the “best-in-class” in the industry—the benchmark;
- the current status of international standards—an additional comparison; and
- the organization’s strategy for improvement—where the organization wants to be.

The maturity model scale is used to quantify and illustrate what is inherently a subjective evaluation. Using the maturity model for a process, multiple parties share this quantification experience by using the same measurement scale. This should help internal audit professionals explain to managers where IT management shortcomings exist and set targets for where they need to be by comparing their organization’s control practices to the best-practice examples. The organization’s business objectives and environment influence the appropriate maturity level for any process. The organization’s dependence on IT, the level of technological sophistication, and the value of its information will determine the appropriate level of control maturity.

The importance of CobiT to internal audit

The IT governance auditing guideline. IT governance is the central focus of CobiT. The Information Systems (IS) Auditing Guideline “IT Governance,” promulgated by ISACA, has been effective for all information systems audits since July 1, 2002. IS Auditing Guidelines provide guidance in applying IS Auditing Standards. Though not mandatory, certified IS auditors are expected to be prepared to justify a departure from the guidelines. This guideline provides a framework for an audit of IT governance in an organization. It discusses the appropriate...
organizational position of the IS auditor who is to undertake the audit, issues to consider when planning the audit, and evidence to review when performing the audit.

Discussion of the need for the guideline begins with several statements drawn from the executive summary in CobiT 3rd Edition that concern the general nature of organizational and management responsibilities. Effective IT governance has become a necessity as organizations have developed critical dependencies on IT.

Reporting on IT governance involves auditing at the highest level in the organization. The IS auditor should confirm that the terms of reference of an IT governance audit state the scope of work, the reporting line to be used where IT governance issues are identified to the highest level of the organization, and the IS auditor's right of access to information. The IS auditor should consider whether his or her organizational status is appropriate for the nature of the planned audit of IT governance. Where this is not considered to be the case, the appropriate level of management should consider the hiring of an independent third party to manage or perform the audit of IT governance.

The Sarbanes-Oxley Act. Sarbanes-Oxley compliance is an important area that makes CobiT extremely vital to internal audit. While it is not specifically targeted at Sarbanes-Oxley compliance, CobiT 4.0 may be used to address this issue. Indeed, one of the CobiT 4.0 byproducts issued by the IT Governance Institute is titled IT Control Objectives for Sarbanes-Oxley. This resource is primarily of interest to governance, assurance, control, and security professionals, including internal auditors and IS auditors. It provides guidance on how to ensure Sarbanes-Oxley compliance for the IT environment based on the CobiT control objectives and addresses the importance of IT in the design, implementation, and sustainability of internal control over disclosure and financial reporting.

Technology is a vital component of every organization's efforts to comply with the Sarbanes-Oxley Act. The importance of IT controls is implicit in the COSO internal control framework, but IT managers and internal auditors need detailed guidelines to establish, document, and/or evaluate their company's controls. CobiT 4.0 is an IT control framework built in part upon the COSO internal control framework. For Sarbanes-Oxley attestation, corporations must be sure that the IT systems that house, move, and transform data are secure. The CobiT framework was designed to address these IT concerns. Thus, CobiT can help IT managers and auditors address specific control objectives for Sarbanes-Oxley compliance.²

Although the SEC suggests that public companies consider the control components of the COSO framework when seeking to comply with the Sarbanes-Oxley Act, neither the SEC nor the Public Company Accounting Oversight Board has openly endorsed a specific IT control framework. Thus, practical questions exist concerning the relationship and alignment between the COSO internal control framework and CobiT 4.0, and guidance is required. Interested readers can refer to the IT Governance Institute's IT Control Objectives for Sarbanes-Oxley and Sally Chan's article "Mapping COSO and CobiT for Sarbanes-Oxley Compliance," which maps COSO internal control components to CobiT domains, though this refers to CobiT 3rd Edition.³

NOTES
1 The IT Governance Institute, CobiT 4.0 (Control Objectives for Information and Related Technology) (Rolling Meadows, IL: The IT Governance Institute, 2005).