

IT Governance Hands-on: Using COBIT to Implement IT Governance¹

By Luc Kordel, CISA, RE, CISSP, CIA, RFA

In the past, running an IT organization as a support function—a function separate and distinct from the business—was a common practice. Now, most IT infrastructure investments and new IT applications span business lines and functions. Some organizations even integrate partners and customers into their internal processes. Therefore, CEOs and CIOs increasingly feel the need for a tighter relationship between IT and the business. But how should they deal with this strategic challenge? The key questions are:

- Is there a framework to guide business and technology management leaders in their efforts to change information technology's role within the organization and to close the gap between IT and the business that IT is supposed to support and drive?
- What are the responsibilities at the board and management levels?
- Is this a governance issue?

The Need to Change IT's Role

This perennial management hot item was discussed in a series of recent articles and studies in leading management journals:

- Consultants Dan Lohmeyer, Sofya Pogreb and Scott Robinson examined the question, "Who is accountable for IT?" and concluded that business leaders are.² To derive full value from their IT investments and use technology as a competitive weapon, organizations should make their business leaders accountable for the return on IT investments by putting them in charge of setting the IT agenda. Moreover, senior executives should have the courage to realign the IT and business organizations to create a partnership between the two sides.
- Research into IT management practices at hundreds of companies around the world has shown that most organizations are not generating optimal value from their IT investments. The most important factor distinguishing top-performing from substandard-performing organizations is the level of leadership by business and senior managers in a handful of key IT decisions. This led Jeanne W. Ross and Peter Weill, research scientists at the MIT Sloan School of Management, to formulate a list of six IT decisions in which leadership responsibility by business and senior managers would generate real value for their IT investments while avoiding IT disasters.³ These six IT decisions relate to strategy and execution. Strategic decisions IT managers should not be making are the level of IT funding as a result of the strategic role of IT, the clear and focused allocation of

IT resources, and the balance between companywide centralized IT capabilities and business-unit IT capabilities. The operational decisions IT managers should not be making are decisions about the service level of IT (how good IT services need to be), the trade-off between security/privacy and convenience, and the business manager accountability for IT projects.

- Consultants Jürgen Laartz, Eric Monnoyer and Alexander Scherdin reported on successes at leading companies where business and IT managers have been working closely together to change the way information technology supports the business.⁴ Although business ownership of IT is in its infancy, business leaders can be in charge of IT decision-making. Even after projects are well underway, they continue to own these IT decisions. In that way, business leaders gain more control over IT assets that directly affect their business and have a greater insight and understanding of what it takes to manage and invest in technology. As a result, they have cut the costs of IT, made it easier to change the business, avoided the constraints of inflexible support systems and increased the participation of business leaders in the management of IT.
- In the highly discussed and criticized article "IT Doesn't Matter," in the *Harvard Business Review*, Nicholas G. Carr, independent author, consultant and *Harvard Business Review* editor-at-large, analyzes the diminishing strategic importance of IT, the vanishing opportunities for IT-based advantage and the commoditization of IT.⁵ Without engaging in the discussion on the potential overestimation of the strategic value of IT and the overspending on technology in the quest for business value, Carr's third new rule for IT management—"focus on vulnerabilities, not opportunities"—highlights the importance of IT risk management. Because IT is critical to the success of an organization, it cannot be delegated solely to IT management. Business managers, as well as IT managers, should focus on potential IT-inspired vulnerabilities.

This selection of leading management literature shares the same basic idea: to be successful, the business side of an organization has to be involved in and committed to what IT does. To deliver the services an organization needs, IT has to be managed by the business as a business. This is the core issue of IT governance.

The Need for IT Governance⁶

If IT is to be managed as a business by the business, the formal means by which management discharges its responsibilities—governance—is also applicable to the management of IT. While governance developments have been

primarily driven by the need for the transparency of organizational risk and the protection of shareholder value, the pervasive use of technology has created a critical dependency on IT that calls for a specific focus on IT governance.

In most organizations, IT is essential to manage the transactions, information and knowledge necessary to initiate and sustain economic activities and to support, sustain and grow the business. As a consequence, the board of directors and top management need to understand the strategic importance of IT and ought to put IT governance firmly on their agenda. The overall objective of IT governance, therefore, is to understand the issues and the strategic importance of IT to enable the organization to sustain its operations and implement the strategies required to extend its activities into the future. At its core, IT governance is concerned about two responsibilities: delivering value and mitigating IT-related risks.

The board and executive management need to extend their governance responsibilities to IT and provide the leadership, organizational structures and processes to ensure that the organization's IT sustains and extends the organization's strategies and objectives.

IT Governance

When properly implemented, IT governance is an organizational structure and set of processes that manage and control the enterprise's IT activities to achieve the enterprise's goals by adding value while balancing risk vs. return over IT. This governance framework should be embedded in the organization and applied to all IT activities and processes (planning, implementation, execution and monitoring). The governance framework encompasses the IT governance environment and five IT governance domains.

IT Governance Environment

IT governance does not occur in a vacuum. Each IT governance implementation takes place in different conditions and circumstances (the IT governance environment) determined by a large set of factors, such as:

- The organization's and the industry's ethics and culture
- The ruling laws, regulations and guidelines, both internal and external
- The mission, vision and values of the organization
- The organization's models for roles and responsibilities
- The organization's and the industry's governance policies and practices
- The organization's business plan and strategic intentions

A good understanding of the business environment, risk appetite, business strategy, IT organization and knowledge of critical IT-related issues and change drivers for the use of IT is essential for a successful IT governance implementation.

IT Governance Domains

These domains represent five management-related issues that map to the following IT governance responsibilities:⁷

- IT strategic alignment: "IT alignment is a journey, not a destination"—Alignment of IT has been synonymous with IT strategy, i.e., does the IT strategy support the enterprise strategy? For IT governance, alignment encompasses more

than strategic integration of the (future) IT organization with the (future) enterprise organization. It also deals with the alignment of IT operations with the current enterprise operations and the ability to build the capabilities necessary to deliver business value. This state of harmony is referred to as alignment.

- IT value delivery: "IT value is in the eye of the beholder"—The basic principles of IT value creation are delivering on time, staying within budget and generating the benefits that were identified and promised. Hence, IT processes must be designed, deployed and operated in an efficient and effective way that meets these delivery expectations and objectives. The value that IT delivers should be aligned directly with the values on which the business is focused, and be measured in a way that transparently shows the impact and contribution of the IT investments in the value creation process of the organization.
- Risk management: "It's the IT alligators you don't see that will get you"—Whereas value delivery focuses on the creation of value, risk management covers the value preservation processes. Internal control requirements and the need to demonstrate sound enterprise governance to shareholders, customers and other stakeholders are the main drivers for increased risk management activities in organizations. Risk management should be a continuous process that starts with the identification of risks (impact on assets, threats and vulnerabilities). Once identified, risks must be mitigated by countermeasures (control), and the residual risk should be formally accepted.
- IT resource management—Resource management is about establishing and deploying the right IT capabilities for business needs. It ensures that an integrated, economical IT infrastructure is provided, wherein new technology is introduced judiciously, and obsolete systems are updated or replaced. It recognizes the importance of people in addition to hardware and software, therefore focusing on maintaining availability, providing training, promoting retention and ensuring competence of key IT personnel.
- Performance measurement: "In IT, if you're playing the game and not keeping score, you're just practicing"—Without establishing and monitoring performance measures, it is unlikely that the previous phases (IT strategic alignment, IT value delivery, risk management and IT resource management) will achieve their desired outcomes. The performance measurement domain closes the loop and provides feedback to the alignment domain by providing evidence that the IT governance initiative is on track and creating the opportunity to take timely corrective measures.

IT Governance Life Cycle

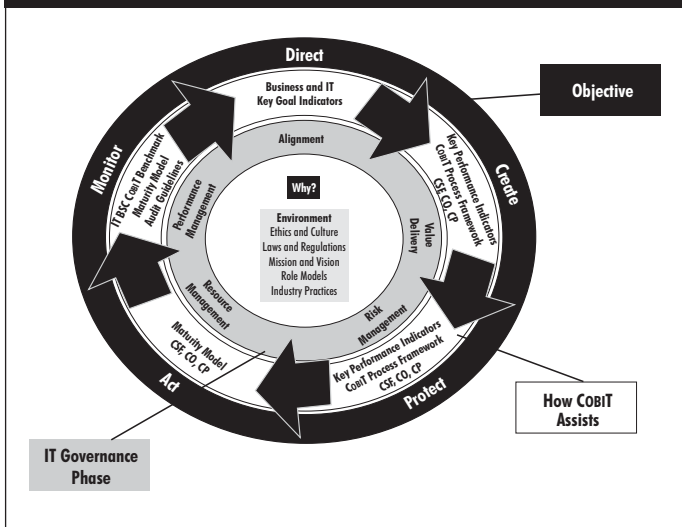
Figure 1 shows the IT governance domains and their related *Control Objectives for Information and related Technology* (COBIT) components in a static way. Because IT governance is considered a life cycle, the IT governance domains can also be represented more dynamically. In the dynamic view of figure 2, the IT governance life cycle is shown as a wheel that can be bootstrapped at any point. The IT Governance Institute (www.itgi.org) advises that the

Figure 1—IT Governance Life Cycle—Static View

IT Governance Domains	Objectives	COBIT Components to Assist	Implementation Tool Kit
ALIGNMENT	DIRECT Ability to build the capabilities necessary to deliver business value	<ul style="list-style-type: none"> • Business and IT key goal indicators 	Documentation and reporting tools
VALUE DELIVERY	CREATE Successful delivery of business value	<ul style="list-style-type: none"> • Key performance indicators • COBIT process framework • Critical success factors • Control objectives • Control practices 	
RISK MANAGEMENT	PROTECT Identification and mitigation risks to preserve value	<ul style="list-style-type: none"> • Maturity model • Critical success factors • Control objectives • Control practices 	IT governance implementation tools
RESOURCE MANAGEMENT	ACT Establishment and deployment of IT capabilities for business needs	<ul style="list-style-type: none"> • IT balanced scorecard • COBIT benchmark • Maturity model • Audit guidelines 	
PERFORMANCE MANAGEMENT	MONITOR Closing the feedback loop to redirect alignment if needed		Information and presentation tools

Source: *IT Governance Implementation Guide*, page 19

Figure 2—IT Governance: A Dynamic View



life cycle is best started from the IT strategic alignment domain. After the bootstrapped start-up, the organization should move into a continuous IT governance cycle. At regular intervals, the feedback loop should be closed; the strategy needs to be monitored and the results measured, reported and acted upon. Generally on an annual basis, the strategy is reevaluated and realigned if required.

To bootstrap the IT Governance cycle, the IT Governance Institute recently published the *IT Governance Implementation Guide*. This book is available at the ISACA Bookstore (www.isaca.org).

IT Governance Implementation Guidance

The objective of the *IT Governance Implementation Guide* is to provide readers with a hands-on methodology for implementing and improving IT governance, using COBIT as the IT control framework. The guide is focused on a generic methodology, covering the following subjects:

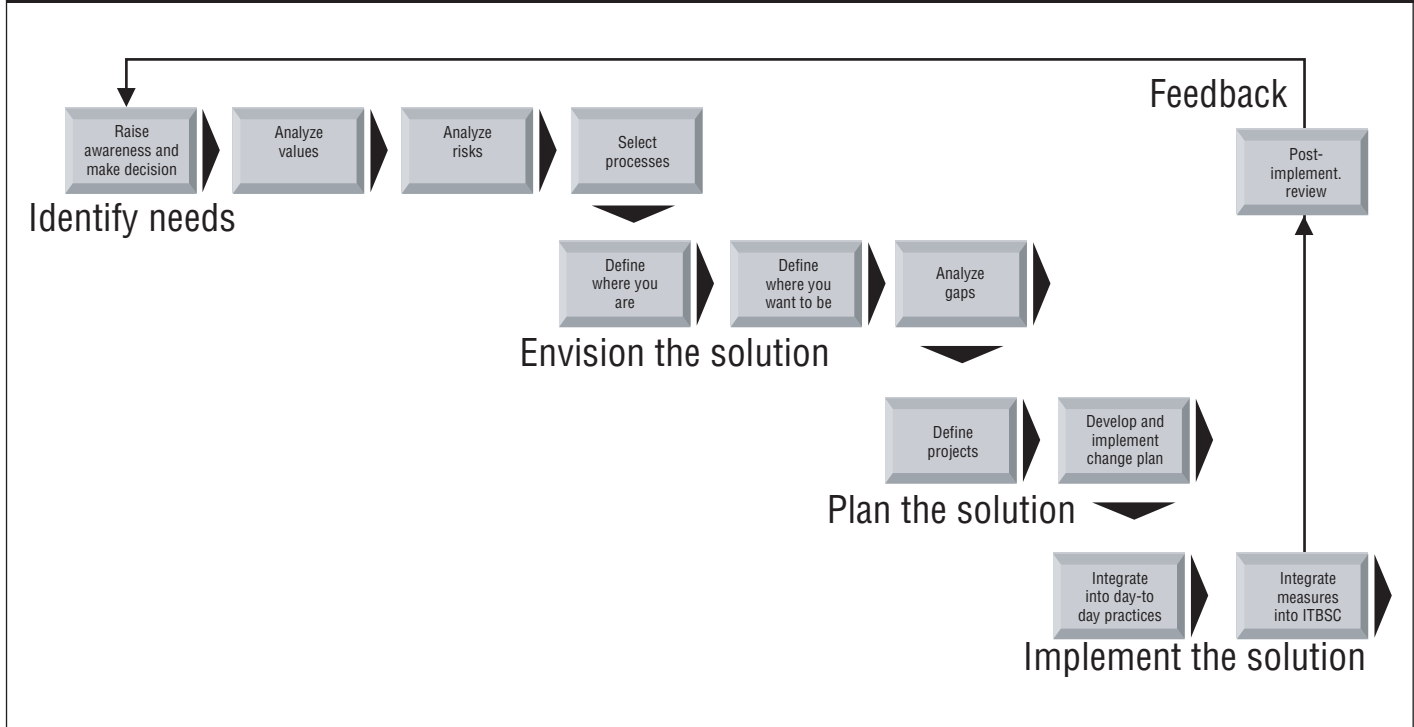
- Why IT governance is important and why organizations should implement it
- The IT governance life cycle
- The COBIT framework
- How COBIT is linked to IT governance and how COBIT enables the implementation of IT governance
- The stakeholders who have an interest in IT governance
- A road map for implementing IT governance using COBIT

Answers for IT Governance Stakeholders

There are many stakeholders interested in IT governance who need to work together to achieve a common business goal. The *IT Governance Implementation Guide* will help them find the answers to their specific questions:

- Executive and board members—How does the board define business goals for IT, implement appropriate IT governance practices and ensure that IT value is delivered and IT-related risks are managed, using the different components from the COBIT IT control framework?
- Business management—How does management define business requirements for IT governance to ensure that value is delivered and risks are mitigated using the different COBIT components?
- IT management—How does IT management deliver IT services as required by the business and directed by the board using the different COBIT components?

Figure 3—IT Governance Implementation Road Map



- IT auditors—How do auditors use the different COBIT components in audit activities to provide independent assurance that IT delivers what it needs to deliver?
- Risk and compliance officers—How do risk managers and compliance officers use the different COBIT components in risk and compliance advisory activities to ensure that new IT-related risks are identified and that IT complies with policies, regulations and laws?

IT Governance Implementation Action Plan: The Road Map to IT Governance

The *IT Governance Implementation Guide* assists the different stakeholders with a detailed road map that can help the organization in implementing its IT governance needs using COBIT. It identifies COBIT components to be leveraged from initial needs all the way through to the implementation of the solution, passing through an envisioning and planning stage. The road map represents a project that can be fairly large and that requires strict project management practices and thorough management involvement and oversight. However, the *IT Governance Implementation Guide* does not elaborate on change and project management skills and practices: the guide is focused on the IT governance and control issues.

The road map (figure 3) is a first pass for implementing IT governance requirements. The road map is a kind of “bootstrap” for IT governance, after which the enterprise should move into a continuous IT governance cycle, reusing the elements of the road map as required.

The Detailed Road Map to IT Governance

The *IT Governance Implementation Guide* presents all 19 steps of the four phases of the implementation action plan in

detail, with navigation aids, detailed tasks and objectives, and inputs. Templates and tools are available to develop and record the results. Because the *IT Governance Implementation Guide* does not elaborate on change and project management skills and practices, the stages of identifying the need, envisioning the solution and planning the solution are more detailed than the actual implementation stage.

Phase 1—Identify Needs (Steps 1.x – 4.x)

The following four steps (11 substeps) are required in the start-up phase of an IT governance implementation project:

- Understand the background of the IT governance initiative, set measurable business objectives for the IT governance implementation project, raise awareness and define a proper project organization.
- Understand the business objectives and how they translate into IT objectives.
- Understand the potential risks and how they could affect IT goals.
- Decide upon the scope of the improvement project, and identify the IT processes to be implemented or improved.

The *COBIT Management Guidelines* offer key goal indicators (KGIs) and critical success factors (CSFs) to help define IT goals. The *COBIT Control Objectives* and *Control Practices* provide guidance on critical control requirements. The information criteria described in the *COBIT Framework* help define the business value and business risk reduction requirements for information. The IT resources help define the resources required to manage delivery of information to meet business value and business risk requirements, and the IT processes help select critical IT processes.

Phase 2—Envision Solution (Steps 5 – 7)

Phase 2 of the road map envisions the solution and is composed of three steps. The current maturity of the selected IT processes (as-is) must be assessed and the appropriate target maturity levels (to-be) are to be set. Based on the maturity attributes in the COBIT *Control Objectives and Control Practices*, the analysis of the gaps between the as-is and to-be positions are translated into improvement opportunities. This phase uses the CSFs and the maturity models from the COBIT *Management Guidelines*.

Phase 3—Plan Solution (Steps 8 – 9)

The third phase of the road map identifies feasible improvement initiatives and translates them into justifiable projects. After approval, these projects should be integrated into an overall improvement strategy with a detailed plan to roll out the solution. The COBIT *Control Objectives and Control Practices* can be used to prioritize improvement opportunities and the COBIT *Management Guidelines*' KPIs and KGIs are available for defining process metrics for the IT and business goals.

Phase 4—Implement Solution (Steps 10 – 12)

As the improvement plan rolls out, the sustainability of the delivery is guaranteed by the feedback provided by the post-implementation review and the monitoring of improvements on the corporate and IT balanced scorecards. In this phase the KGIs and KPIs from the COBIT *Management Guidelines* can be used to establish an IT balanced scorecard and to document a post-implementation review.

IT Governance Implementation Tool Kit

The hands-on methodology presented in the *IT Governance Implementation Guide* is supported by the Supplemental Tools and Materials CD-ROM. The CD-ROM contains a variety of resources for implementing effective IT governance initiatives, including documentation and reporting tools, IT governance implementation tools and helpful information and presentation tools. The CD-ROM can be found at the back of the *IT Governance Implementation Guide*. The tools are available in Microsoft Word, PowerPoint, Excel or Adobe Acrobat format.

Documentation and Reporting Tools

IT Governance Implementation Templates

This PowerPoint document contains example templates that can be used to support the IT governance implementation activities described in the *IT Governance Implementation Guide*:

- The project initiation template contains a project initiation plan checklist.
- The organization plan template and the resource plan template are examples of how to document the organization of an IT governance initiative (responsibilities, project team structure and resource plan, stakeholders, and interested or affected parties) and can be used as checklists.
- The framework template serves as an example of how to document the various elements of the control framework used.

- The communication plan template helps to document the IT governance awareness plan.
- IT heat maps are cross-references between business goals (e.g., reduce costs, launch new product, improve trust image), corresponding IT goals (e.g., reduce headcount, manage availability risks, develop and test new modules, manage project delivery risks, reduce security incidents) and IT information criteria, IT resources or IT processes, indicating which different criteria, resources or processes are affected by which goals and to what extent (low, medium or high).
- The IT issues template is used to report issues, with the top part building up the scope and background explanations, and the lower part of the template reporting concerns, grouped by IT domain, and potentially IT process.
- The IT risks template provides an example and checklist on how to document the IT risk profile, operational risks and project risks.
- The capability worksheet documents the as-is status and the to-be improvements.
- The IT process capability maturity scorecard documents the maturity levels of IT processes.
- The opportunity worksheet, opportunity grid and change plan template document visualize and prioritize the possible areas that will need to be dealt with as a part of the IT governance implementation action plan.
- IT balanced scorecard templates are also included.

These templates are intended to be generic and simple to use and can be tailored to suit a particular organization. The Excel objects within some of the templates are modifiable.

Reporting Techniques

The communication of results from IT governance implementation projects can be greatly enhanced through the use of graphics and colors to convey key messages to management. To raise awareness and enable a focus on important topics that are otherwise often lost in lengthy written reports, the slides included in the Supplemental Tools and Materials CD-ROM provide some examples of:

- Boston squares to highlight high-priority projects with high potential for success and high impact on the business
- Rising star charts as the as-is and to-be maturity model recording and reporting tool based on maturity model attributes
- Traffic light reports and heat maps
- IT process capability maturity reporting through bar charts and spider charts

IT Governance Implementation Tools

Diagnostic Tools

These diagnostic tools are useful for attracting management's attention and raising their awareness by analyzing, understanding, documenting and communicating important aspects of the organization's IT control environment, current management concerns and risks:

- Management awareness diagnostics 1—This global diagnostic ranks IT process importance (how important for the organization) and performance (how well it is done) and records whether the process is audited, formalized (is there a contract, an SLA or a clearly documented procedure?) and accountable, and who performs it.

- Management awareness diagnostics 2—This detailed diagnostic (at the IT process level) assesses the process importance and checks nine key issues about the way the process is being managed (accountability, formality, performance, responsibility, direction, measurement, audit, control weaknesses and technology vulnerabilities).
- The themes-to-controls diagnostic tool—It maps governance themes and current management concerns to the COBIT IT processes and detailed control objectives. This tool helps in selecting the processes and controls that are likely to be relevant to a particular theme. Governance themes are strategic alignment, value delivery, risk management, IT resource management and performance management. Current management concerns are cost optimization, service delivery, selective outsourcing, security, enterprise architecture, system integration, prioritizing and planning, application controls and application security.
- The themes-to-risk-factors diagnostic tool—This tool maps 77 risk factors commonly found in IT environments with the two sets of themes mentioned in the preceding tool. This tool helps in understanding how risks and themes interrelate.
- The maturity measurement tool—It provides a pragmatic approach to maturity measurement for an IT process. It provides a template to deconstruct the maturity descriptions from the COBIT *Management Guidelines* into a number of statements/attributes per maturity level. Additionally, a weight factor can be assigned to each maturity attribute and maturity level (depending on the organization).

Risk Analysis Approach

This document draws a generally accepted approach for risk analysis in IT based on COBIT's audit guidelines, which can be applied in step three of phase one of the implementation road map (analyze risks).

The model starts from the valuation of assets, which, in the COBIT framework, consists of the information that has the required criteria to help achieve the business objectives (including all the resources necessary to produce that information). The next step is the vulnerability analysis, which looks at the importance of the information criteria in the process under review, i.e., if a business process is vulnerable to integrity loss, then specific measures are required. Next, one looks at threats, i.e., that which can exploit a vulnerability. The probability of the threat, the degree of vulnerability and the severity of the impact are combined to conclude on the risk assessment. This is followed by the selection of countermeasures (controls) and an evaluation of their effectiveness, which also identifies residual risk that should be translated into business and financial consequences. The final outcome is an action plan that closes the feedback loop.

IT Balanced Scorecard⁸

The IT balanced scorecard is a very important mechanism for managing and aligning IT. Therefore, step 11 of the implementation road map refers to the establishment of an IT balanced scorecard. In the CD-ROM, an example IT balanced scorecard is provided, along with a high-level implementation process to create it.

Balanced scorecards translate strategy into action to achieve goals with a performance measurement system that goes beyond conventional accounting, by measuring those relationships and knowledge-based assets necessary to compete in the information age: customer focus, process efficiency and the ability to learn and grow. At the heart of these scorecards is management information supplied by the IT infrastructure. IT also enables and sustains solutions for the actual goals set in the financial (enterprise resource management), customer (customer relationship management), process (intranet and workflow tools) and learning (knowledge management) dimensions of the scorecard.

Because of its criticality, IT needs its own scorecard. Defining clear goals and good measures that unequivocally reflect the business impact of the IT goals is a challenge and needs to be resolved in cooperation with the different governance layers in the enterprise. The linkage between the business balanced scorecard and the IT balanced scorecard is a strong method of alignment. Many of the outcome measures of IT influence how well the enterprise is doing and, therefore, are performance measures for the enterprise. It is equally vital to stress that the balanced scorecard should demonstrate the value that IT delivers to the enterprise.

Information and Presentation Tools

COBIT Presentations

The CD-ROM contains a selection of seven COBIT presentations that can be used selectively to support IT governance presentations and that can be tailored to reflect an organization's specific circumstances and requirements:

- Three general COBIT presentations
- Case studies (a complete and continuously updated list of case studies is available at www.isaca.org/cobit)
- Mapping of COBIT to other standards (e.g., COBIT processes to ITIL)
- Results of two surveys (IT governance maturity survey and IT control maturity survey)

COBIT Mappings

The tool kit also includes a series of three detailed mappings that clarify the relationship of COBIT to other international standards:

- COBIT processes to COSO components
- COBIT control objectives to COSO components
- ISO17799 to COBIT control objectives and processes

COBIT Frequently Asked Questions (FAQ)

This Word document contains a list of frequent questions and corresponding answers regarding the use of COBIT, its goals, its structure, etc. A continuously updated list of FAQs can be found on COBIT Online.

Possible Future Developments of IT Governance Tools

Because the multitude of tools in the CD-ROM are built on and designed for the Microsoft Office System, the tool kit is a possible candidate to be transformed into an Office Solution Accelerator for IT governance. In the same manner, the announced Office Solution Accelerator for Business Scorecards—adapted for IT balanced scorecards—can be used to gain visibility into key IT performance metrics.

Another Important IT Governance Publication

*Strategies for Information Technology Governance*⁹ by Idea Group Publishing is a recent academic publication giving an overview of the best in IT governance. As stated in its preface,¹⁰ the book is aimed at improving the understanding of IT governance and its structures, processes and relational mechanisms. This publication brings together 14 papers on IT governance written by academics and practitioners from nine different countries including Belgium, Canada, Finland, Greece, The Netherlands, Norway, Spain, UK and US.

The 14 chapters are grouped in four sections:

- Section I, Introducing the IT Governance Frameworks, consists of three chapters:
 1. Structures, Processes and Relational Mechanisms for IT Governance
 2. Integration Strategies and Tactics for Information Technology Governance
 3. An Emerging Strategy for E-business IT Governance
- Section II, Performance Management as IT Governance Mechanism, reviews IT governance mechanisms, including balanced scorecards, business-IT alignment maturity assessment models, ROI measurement and technical IT measurements. This part consists of six chapters:
 4. Assessing Business-IT Alignment Maturity
 5. Linking the IT Balanced Scorecard to the Business Objectives at a Major Canadian Financial Group
 6. Measuring and Managing E-business Initiatives Through the Balanced Scorecard
 7. A View on Knowledge Management: Utilizing a Balanced Scorecard Methodology for Analyzing Knowledge Metrics
 8. Measuring ROI in E-commerce Applications: Analysis to Action
 9. Technical Issues Related to IT Governance Tactics: Product Metrics, Measurements and Process Control
- Section III, Other IT Governance Mechanisms, describes other mechanisms including roles and responsibilities within the IT organization, the control objectives and management guidelines of COBIT, and the IT outsourcing solution. This section consists of three chapters:
 10. Managing IT Functions
 11. Governing Information Technology Through COBIT
 12. Governance in IT Outsourcing Partnerships
- Section IV, IT Governance in Action, describes the application of IT governance structures in two case studies:
 13. The Evolution of IT Governance at NB Power
 14. Governance Structures for IT in the Healthcare Industry

Because of the mix of theoretical models, practices and mechanisms regarding IT governance, this book is highly recommended management literature for all managers engaged in the oversight and the management of information technology.

Conclusion: It Is a Method, Not the Solution

The *IT Governance Implementation Guide* assists the different IT stakeholders with a generic methodology and a detailed road map that can help them in starting up, implementing, maintaining and improving a continuous IT governance life cycle. Because the guidance builds extensively

on all of the COBIT components, it is assumed that the readers of the *IT Governance Implementation Guide* are already familiar with COBIT. The guide is supported by the Supplemental Tools and Materials CD-ROM and contains a variety of resources, including documentation and reporting tools, IT governance implementation tools and information and presentation tools.

Because the IT governance implementation methodology provides only generic guidance, the IT governance implementation road map presented in this guide is not prescriptive and should be tailored to the needs of the organization applying it. The guide does not provide the solution. It provides a hands-on efficient method for implementing IT governance using COBIT.

References

- Carr, Nicholas G.; "IT Doesn't Matter," *Harvard Business Review*, May 2003, pp. 41-49
- Guldentops, Erik; "Boards and IT—Unleash the Value, Put a Leash on the Risks," *Information Systems Control Journal*, volume 2, 2002
- Guldentops, Erik; "Knowing the Environment: Top Five IT Issues," *Information Systems Control Journal*, volume 4, 2002, pp. 15-16
- Hardy, Gary; "Make Sure Management and IT are on the Same Page: Implementing an IT Governance Framework," *Information Systems Control Journal*, volume 3, 2002
- IT Governance Implementation Guide*, IT Governance Institute, 2003, p. 58, www.itgi.org
- Board Briefing on IT Governance, 2nd Edition*, IT Governance Institute, 2003, p. 64, www.itgi.org
- Laartz, Jürgen; Eric Monnoyer; Alexander Scherдин; "Designing IT for Business: When Business and Computer People Put Their Heads Together, They Can Transform a Company's IT Architecture," *The McKinsey Quarterly*, number 3, 2003, pp. 76-86
- Lohmeyer, Dan; Sofya Progreb; Scott Robinson; "Who's Accountable for IT? Business Leaders—That's Who," *The McKinsey Quarterly*, number 4, 2002, pp. 38-47
- Monnoyer, Eric; "What CEOs Really Think About IT," *The McKinsey Quarterly*, number 3, 2003
- Ross, Jeanne W.; Peter Weill; "Six IT Decisions Your IT People Shouldn't Make," *Harvard Business Review*, November 2002, pp. 84-91
- Van Grembergen, Wim (Editor), *Strategies for Information Technology Governance*, Idea Group Publishing, 2004

Endnotes

- ¹ The information in this article is based primarily on the text of the *IT Governance Implementation Guide*, IT Governance Institute, USA, 2003.
- ² Lohmeyer, Dan; Sofya Progreb; Scott Robinson; "Who's Accountable for IT? Business Leaders—That's Who," *The McKinsey Quarterly*, number 4, 2002, pp. 38-47

³ Ross, Jeanne W.; Peter Weill; "Six IT Decisions Your IT People Shouldn't Make," *Harvard Business Review*, November 2002, pp.84-91

⁴ Laartz, Jürgen; Eric Monnoyer; Alexander Scherдин; "Designing IT for Business: When Business and Computer People Put Their Heads Together, They Can Transform a Company's IT Architecture," *The McKinsey Quarterly*, number 3, 2003, pp. 76-86

⁵ Carr, Nicholas G.; "IT Doesn't Matter," *Harvard Business Review*, May 2003, pp. 41-49

⁶ The information in this section of the article is based on the chapter "Introduction to IT Governance" of the *IT Governance Implementation Guide* and the *Board Briefing on IT Governance, 2nd Edition*, IT Governance Institute, 2003.

⁷ The description of the IT governance domains is based on chapter 11: Governing Information Technology Through COBIT, by Erik Guldentops, in *Strategies for Information Technology Governance*, Idea Group Publishing, 2004, edited by Wim Van Grembergen.

⁸ The description of the IT balanced scorecard is based on chapter 11: Governing Information Technology Through COBIT, by Erik Guldentops, in *Strategies for Information Technology Governance*, Idea Group Publishing, 2004, edited by Wim Van Grembergen.

⁹ Van Grembergen, Wim (Editor), *Strategies for Information Technology Governance*, Idea Group Publishing, 2004

¹⁰ The information in this section of the article is based on the preface of *Strategies for Information Technology Governance*.

Luc Kordel, CISA, RE, CISSP, CIA, RFA

is an IT audit, control and security professional with more than 15 years of experience and a lecturer in IT/IS management, IT audit and IT security at the graduate level. He was a member of the development team of the *IT Governance Implementation Guide*. Kordel is one of the founding members of the ISACA Belux Chapter and serves as the ISACA Belux CISA coordinator. His latest domain of interest is forensic auditing and its relation to IT control and IT security.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the *Information Systems Audit and Control Association, Inc.*. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the *Information Systems Control Journal*.

Opinions expressed in the *Information Systems Control Journal* represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors' employers, or the editors of this Journal. *Information Systems Control Journal* does not attest to the originality of authors' content.

© Copyright 2004 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org