An IT Assurance Framework for the Future

by John W. Lainhart IV

Even though computers and the Internet have changed nearly every facet of business management, two aspects have remained steadfast. Executives always will need to make educated, rational business decisions and stakeholders will require solid assurance regarding enterprise risk and control. As a result, accountants, auditors and business consultants must continue to adapt to the constantly changing environment and increase their knowledge about monitoring information and related systems within their organizations.

The AICPA has even identified information technology (IT) as a core service and core competency incorporated into its vision process. The organization views IT as a long-range initiative to reposition the accounting profession for the 21st century and is dedicating increased resources toward technology.

Business and IT Issues Integrated

Many of the issues currently facing enterprise managers go back to the dawn of modern business. What brings them to the forefront now is the increased pace, expectations and vulnerabilities resulting from integrating IT and the Internet into the traditional auditing mix.

The Gartner Group recently issued a report on its Web site noting that the worldwide business-to-business (B2B) eCommerce market is forecast to grow from $403 billion in 2000 to $7.29 trillion in 2004. This indicates that, now more than ever, IT must be aligned with and enable enterprises to take full advantage of information. By so doing, enterprise management can maximize its IT benefits, capitalize on business opportunities and gain a competitive advantage.

As enterprises increasingly take advantage of the benefits of technology, they must also recognize the need to understand and manage the associated risks.

As enterprises increasingly take advantage of the benefits of technology, they must also recognize the need to understand and manage the associated risks. Businesses have to integrate their IT with business strategies to attain their business objectives. This has generated a new area of accountability called IT governance.

IT governance functions in a similar manner as enterprise governance, although in a more focused arena. Like an organization itself, IT also is governed by good (or best) practices. For IT, these practices are designed to ensure that the enterprise’s IT resources are used responsibly, its risks are managed appropriately and its information and related technology support its business objectives.

With an appropriate IT governance plan in place, organizations can confidently address major business issues such as ERP (enterprise resource planning) and electronic commerce. An effective IT governance plan can help an enterprise:

- Assure the security, reliability and integrity of its strategic information.
- Protect its investment in IT, including systems and networks
- Ensure the appropriate management of information assets, which often are directly responsible for the success and survival of the enterprise itself.

One entity focused on aligning business objectives with IT objectives is the state of Oregon, which adopted an IT governance tool called COBIT® (Control Objectives for Information and Related Technology) as its statewide enterprise control standard. The Oregon State Controller’s Division stated that all IT related management and investment activities, both in the central agencies and field agencies, fall under the scope of COBIT.

According to John Radford, Oregon state controller, “COBIT represents a significant step forward in managing Oregon’s approach to IT governance and control. No other IT control standard gives management such a high degree of comprehensive coverage and flexibility. The auditing aspect gives us the approach we need to link to public accountability.”

COBIT Basics

But what exactly is COBIT®? Now in its third edition, COBIT is a breakthrough tool that helps enterprises...
balance IT risk and investment in controls. It includes a comprehensive framework of control objectives based on 41 international source documents, providing a global perspective and a best practice point of view.

Business orientation is the main theme of COBIT. It is designed not only to be employed by users and auditors, but also, and more importantly, as a comprehensive checklist for business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls. COBIT provides a tool for the business process owner that facilitates the discharge of this responsibility.

Furthermore, management must satisfy the quality, fiduciary and security requirements for its information, as for all assets. Management must also optimize the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve the organization's objectives, management must establish an adequate system of internal control. Thus, an internal control system must be in place to support the business processes and it must be clear how each individual control activity satisfies the information requirements and impacts the resources. Impact on IT resources is highlighted in COBIT, together with the business requirements for effectiveness, efficiency, confidentiality, integrity, availability, compliance and reliability of information that need to be satisfied.

COBIT starts from a simple and pragmatic premise:

In order to provide the information that the organization needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

COBIT describes a set of 34 Control Objectives, one for each of the IT processes, grouped into four domains: planning and organization, acquisition and implementation, delivery and support, and monitoring.

- **Planning and Organization**—This domain covers strategy and tactics and the identification of the way IT can best contribute to the achievement of the business objectives.

  - One entity focused on aligning business objectives with IT objectives is the state of Oregon, which adopted an IT governance tool called COBIT® (Control Objectives for Information and Related Technology) as its statewide enterprise control standard.

- **Acquisition and Implementation**—To realize the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure that the life cycle is continued for these systems.

- **Delivery and Support**—This domain is concerned with the actual delivery of required services, which range from traditional operations over security and continuity aspects to training. This domain includes the actual processing of data by application systems.

- **Monitoring**—All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain thus addresses management's oversight of the organization's control process and independent assurance provided by internal and external audit or obtained from alternative sources.

This structure covers all aspects of information and the technology that supports it. By addressing these 34 Control Objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

Released by the IT Governance Institute in 2000, www.itgovernance.org, and the Information Systems Audit and Control Foundation (ISACF), www.isaca.org, the COBIT 3rd Edition package consists of an Executive Summary, a Framework, high-level and detailed Control Objectives, Audit Guidelines, an Implementation Tool Set and in depth Management Guidelines. All portions of COBIT, except for the Audit Guidelines, are available to the public as a free download from the Information Systems Audit and Control Association® (ISACA™) Web site www.isaca.org. (The Audit Guidelines are available on a complimentary download basis to ISACA members.) In addition, all sections, including the Audit Guidelines, are available in a six-book/CD-ROM package.

Specifically, COBIT is comprised of:

- **Executive Summary**, which provides an overview of COBIT's issues and foundational premise.

- **COBIT Framework**, which describes in detail the high-level IT control objectives, and identifies the business requirements for information and IT resources primarily impacted by each control objective.

- **Control Objectives**, which contains statements of the desired results or purposes to be achieved by implementing 318 specific, detailed control objectives.
Audit Guidelines, which contain suggested audit steps corresponding to each of the high-level IT Control Objectives.

Implementation Tool Set, which provides lessons learned from organizations that successfully applied COBIT in their work environments and several tools to help management assess its control environment related to information and IT resources.

Management Guidelines, which contain critical success factors, key goal indicators, key performance indicators and maturity models. The Management Guidelines are intended to provide management tools to assess and measure organizations’ IT environment against COBIT's 34 IT processes.

Brief COBIT Case Studies

In addition to the state of Oregon, other organizations have customized COBIT for their unique needs.

Sears, Roebuck & Co. (Hoffman Estates, Ill.), was an early adopter of the COBIT model and used its principles to better educate its internal clients about internal controls. COBIT clicked because it presents control activities in a manageable and definable structure in line with management objectives for the business. According to the Sears team, COBIT’s business slant—coupled with its in-depth, step-by-step instructions—make it a unique and valuable tool.

Fidelity Investments (Boston, Mass.), found that COBIT directly addresses the challenges faced by its CIO and other executives by continually improving IT systems. COBIT moved the process forward by offering a baseline of IT controls that relate directly to Fidelity’s business objectives.

Office of the State Auditor of Massachusetts, has used COBIT extensively in audit selection, on individual engagements and for substantiating results. The IT audit division has performed integrated, financial-related, operational and IT audits in a multi-platform environment. After completing these audits, the team developed a series of COBIT-based matrices to assist the auditors in pre-audit work involving identifying high risk IT processes and assessing the IT control environment. COBIT’s focus on control objectives and how they support the business organization has facilitated audit management’s efforts to move away from checklist auditing.

During entrance conferences, Massachusetts audit teams could reference COBIT as one of their primary audit criteria. This authoritative source lent credibility to the review criteria, and when shared with the auditee, provided new opportunities for constructive audit work and helped auditees understand the basis of the review from the start. With auditees more prepared for upcoming audits, they could better relate to and interpret auditors’ requests for information and subsequent recommendations. COBIT also helped entry level auditors gain an understanding of IT processes and detailed control objectives.

United States Federal Financial Institutions Examination Council (FFIEC), adopted a revised Uniform Rating System for Information Technology (URSIT). The FFIEC published the revised rating system in the United States Federal Register on Jan. 20, 1999 (64 FR 3109). This revised system is to be used in IT examinations of all banks and data processing service providers. URSIT uses COBIT as a guideline for IT controls and is to be implemented in future IT examinations of all banks and data processing service providers. While URSIT is implemented within the Federal Reserve System, it affects all financial institutions that are participating in the Federal Deposit Insurance Corporation (FDIC).

Daimler-Chrysler has incorporated the COBIT framework and control objectives into its internal controls standards database for use in audit planning throughout the world by IT auditors based in Germany and the United States.

United States Federal Information Systems Control Audit Manual, includes COBIT references in every section. This manual is used by all internal auditors in the United States federal government. The document can be obtained from the United States General Accounting Office (Publication: GAO/AIMD-12.19.6).

United States Critical Infrastructure Assessment Office, has defined a vulnerability assessment framework for federal government agencies that references COBIT as the basis for its IT control framework. The guidelines are currently for U.S. agencies, but are equally applicable to private enterprises and international organizations.

IT Governance Self-Assessment

COBIT provides an additional tool to help companies get started evaluating their own IT governance systems. The IT Governance Self-Assessment checklist helps auditors to determine for each of the COBIT processes:

- How important the process is for their business objectives.
- Whether the process is well performed (The combination of importance and performance provide a strong indicator of risk.)
- Who performs the process and who is accountable for the process? (Whether accountability is unequivocal and accepted.)
- Whether the process and its control are formalized. (Is there a contract for an outsourced activity or a clear set of documented procedures for an internal process?)
- Whether the process is audited.

Completion of this checklist heightens management's awareness of the combination of risk indicators, degree of formality and clarity of responsibility and accountability. High risk indicators combined with "don't know" answers relay a strong message of concern.

Management can concentrate on the areas of high risk identified through auditors’ assessments and then use COBIT's high-level and detailed control objectives to determine cost-effective
### The IT Governance Self-Assessment Checklist

<table>
<thead>
<tr>
<th>Importance</th>
<th>Risk</th>
<th>Performance</th>
<th>Who Does it?</th>
<th>Audited</th>
<th>Formality</th>
<th>Who is accountable?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Importance—how important for the organization, on a scale from 1 (not at all) to 5 (very)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Performance—how well it is done, from 1 (don’t know or badly) to 5 (very well)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Audited—Yes, No or ?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Formality—is there a contract, an SLA or a clearly documented procedure? (Yes, No or ?)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Accountable—Name or “don’t know”</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### COBIT’s Domains and Processes

**PLANNING AND ORGANIZATION**

- **PO1** Define a Strategic IT Plan
- **PO2** Define the Information Architecture
- **PO3** Determine the Technological Direction
- **PO4** Define the IT Organization and Relationships
- **PO5** Manage the IT Investment
- **PO6** Communicate Management Aims and Direction
- **PO7** Manage Human Resources
- **PO8** Ensure Compliance with External Requirements
- **PO9** Assess Risks
- **PO10** Manage Projects
- **PO11** Manage Quality

**ACQUISITION AND IMPLEMENTATION**

- **A11** Identify Solutions
- **A12** Acquire and Maintain Application Software
- **A13** Acquire and Maintain Technology Architecture
- **A14** Develop and Maintain IT Procedures
- **A15** Install and Accredit Systems
- **A16** Manage Changes

**DELIVERY AND SUPPORT**

- **DS1** Define Service Levels
- **DS2** Manage Third-Party Services
- **DS3** Manage Performance and Capacity
- **DS4** Ensure Continuous Service
- **DS5** Ensure Systems Security
- **DS6** Identify and Attribute Costs
- **DS7** Educate and Train Users
- **DS8** Assist and Advise IT Customers
- **DS9** Manage the Configuration
- **DS10** Manage Problems and Incidents
- **DS11** Manage Data
- **DS12** Manage Facilities
- **DS13** Manage Operations

**MONITORING**

- **M1** Monitor the Processes
- **M2** Assess Internal Control Adequacy
- **M3** Obtain Independent Assurance
- **M4** Provide for Independent Audit

Information: Systems Audit© and Control Foundation™

---

22 · The Ohio CPA Journal · January-March, 2001
means for mitigating these risks. As a result, the enterprise’s IT governance is enhanced and auditors provide true value-added benefits to the entire enterprise.

**Management-Focused Framework**

COBIT 3rd Edition includes new tools to help accounting and financial professionals monitor the union of business processes and information systems. For example, a new business-oriented section has been developed in the generally accepted form of critical success factors (CSF), key goal indicators (KGI), key performance indicators (KPI) and maturity models. These Management Guidelines help professionals assess and benchmark their organization’s IT environment. They also help answer management’s frequent questions about the right level of control needed to support the enterprise’s objectives. The tools include:

- **CSFs**—define the most important issues and actions for management to address for achieving control over and within its IT processes. CSFs are management-oriented guidelines that identify the most important things to do strategically, technically, organizationally or procedurally.

- **KGIs**—are measures that inform management if an IT process is achieving its business requirements. These are the types of measures that management likes to see on its “dashboard.” KGIs usually are expressed in terms of the information criteria:
  - Availability of information the business needs
  - Absence of integrity and confidentiality risks
  - Cost-efficiency of processes and operations
  - Confirmation of reliability, effectiveness and compliance

- **KPIs**—are measures of how well the process is performing. They are process oriented, but IT driven. KPIs are expressed in terms of capabilities, practices and skills that enable the process to achieve its goals.

- **Maturity Models**—help the organization perform self-assessments and measure how well management processes are developed and provide a theoretical measurement scale for each of COBIT’s 34 IT processes by allowing management to map the:
  - Requirements of the most stringent emerging international standards/regulations
  - Current status of the organization
  - Current status of best-in-class organizations in the industry
  - Organization’s strategy for targeted improvement

To sum up all these acronyms and understand how they interact within the Management Guidelines, CSFs suggest what needs to be done based on the choices made in the Maturity Models, while monitoring through KPIs whether the enterprise will likely reach the IT process goal set by the KGI.

Monitoring and controlling an enterprise is a continually changing challenge and multifaceted opportunity. Accounting professionals must make positive, measurable contributions to the success of their client or enterprise or else risk not being a part of the enterprise as it moves forward.

---

**John W. Lainhart IV** is a partner in the Washington consulting practice of PricewaterhouseCoopers in Washington, DC. Prior to joining PwC, Lainhart was Inspector General of the U.S. House of Representatives and was responsible for conducting periodic audits of the financial and administrative functions of the House and joint entities. Lainhart established the Office of the Inspector General (OIG) and carried out the first House audit, which helped to identify $20 million in potential savings or cost avoidance. He also provided management advisory services related to various systems.