

SARBANES-OXLEY AND IT GOVERNANCE: NEW GUIDANCE ON IT CONTROL AND COMPLIANCE

MARIOS DAMIANIDES

Having weathered the storm of legislation, such as the Sarbanes-Oxley Act of 2002, that broke in the wake of corporate wrongdoing, enterprises are beginning to rebound and get back to new (or maybe it is back to the old) “business as usual.” As they redirect their focus from compliance as a necessary evil to compliance as a competitive advantage, and capitalize on the recovering economy, companies are also turning a spotlight on governance and controls over information technology.

This focus will only increase as IT continues to grow in importance to organizations, both through day-to-day operations and also as a competitive advantage. Although there are mixed economic signals following years of record declines, IT spending is expected to achieve five percent growth in 2004, to U.S. \$916 billion, according to the *IT Black Book* published by the IDC. With IDC forecasts based on relatively conservative economic assumptions, Stephen Minton, IT spending analyst at IDC said, “If the recent announcement of surging economic growth in the U.S. is sustained, and the gradual improvement in international economies continues, we can look forward to a further uptick in IT spending expectations.”

Along with this economic improvement, IT professionals are facing even greater challenges to meet raised expectations to provide accurate, visible, and timely information, while ensuring the protection, privacy, and security of their organizations’ information assets. Executives and stakeholders require IT to deliver business value, generate a return on investment, and move from efficiency and productivity gains toward value creation and business effectiveness.

Security remains a leading area of interest, with 88 percent of senior business executives rating it as a high priority for their company, according to a survey from the Council on Competitiveness. Security initiatives are becoming more

IN THIS ISSUE

- **Sarbanes-Oxley and IT Governance: New Guidance on IT Control and Compliance**
- **The Audit/Security Alliance**

Editor
RICHARD O'HANLEY

Editor Emeritus
BELDEN MENKUS, CISA



highly valued as a good investment, and 71 percent of those surveyed believe upgraded security will yield positive returns on investment due to increased business continuity and efficiency. This was a dramatic increase from the previous year, when only 24 percent of respondents thought that security initiatives would create a positive return.

The prominent role of IT in creating business value has accelerated the establishment of the concept of IT governance as a high priority for boards of directors and executive management. In response, IT governance practices need to focus on ensuring that the expectations of IT are met and that IT risks are mitigated. An effective IT governance program will help organizations understand the issues and risks surrounding the strategic importance of IT, ensure that IT can sustain operations, and help enable companies to use IT for competitive advantage.

*IT GOVERNANCE
PRACTICES NEED
TO FOCUS ON
ENSURING THAT THE
EXPECTATIONS OF
IT ARE MET AND
THAT IT RISKS ARE
MITIGATED.*

INCREASED REGULATIONS AND CONTROLS

The financial misdeeds and resulting scandals that ravaged some major, high-profile organizations in recent years sent shockwaves that damaged investor confidence and spawned new legislation such as the Sarbanes–Oxley Act. Sarbanes–Oxley focuses on enhancing corporate governance through measures that will augment internal checks and balances and, ultimately, strengthen corporate accountability. It clearly delineates the rules for accountability and supports a simple premise: good corporate governance and ethical business practices are no longer optional — they are the law.

Sarbanes–Oxley makes executives of public companies explicitly responsible for establishing, evaluating, and monitoring the effectiveness of internal control over financial reporting and disclosure. IT will be crucial to achieving this objective and establishing the foundation for a sound internal control environment.

“With the future of capital markets — the very foundation of the economy — at stake, the need to link sound corporate

If you have information of interest to EDPACS, contact Richard O’Hanley, Editor, Auerbach Publications, 29 W. 35th Street, 7th Floor, New York, NY 10001 (ro’hanley@crcpress.com). EDPACS (ISSN 0736-6981) is published monthly by Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431. Periodicals postage is paid at Boca Raton and additional mailing offices. The subscription rate is \$245/year in the U.S. Prices elsewhere vary. Printed in USA. Copyright 2004 EDPACS is a registered trademark owned by CRC Press LLC. All rights reserved. No part of this newsletter may be reproduced in any form — by microfilm, xerography, or otherwise — or incorporated into any information retrieval system without the written permission of the copyright owner. Requests to publish material or to incorporate material into computerized databases or any other electronic form, or for other than individual or internal distribution, should be addressed to Auerbach Publications, Editorial Services, 2000 NW Corporate Blvd., Boca Raton, FL 33431. All rights, including translation into other languages, reserved by the publisher in the U.S., Great Britain, Mexico, and all countries participating in the International Copyright Convention and the Pan American Copyright Convention. Authorization to photocopy items for internal or personal use, or the personal or internal use of specific clients may be granted by CRC Press LLC, provided that \$20.00 per article photocopied is paid directly to Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923 USA. The fee code for users of the Transactional Reporting Service is ISSN 0736-6981/04/\$20.00+\$0.00. The fee is subject to change without notice. For organizations that have been granted a photocopy license by the CCC, a separate system of payment has been arranged. Product or corporate names may be trademarks or registered trademarks, and are only used for identification and explanation, without intent to infringe. POSTMASTER: Send address change to EDPACS, Auerbach Publications, CRC Press LLC, 2000 NW Corporate Blvd., Boca Raton, FL 33431.

governance with effective control activities has never been greater,” said Christopher Fox, CA, PricewaterhouseCoopers LLP. “Forward-thinking companies and executives are seizing the opportunity and turning compliance into a competitive advantage. Companies that fail to act may pay a heavy price.”

Fox, along with Paul Zonneveld, CISA, CA, Deloitte, co-wrote “IT Control Objectives for Sarbanes–Oxley: The Importance of IT in the Design, Implementation and Sustainability of Internal Control over Disclosure and Financial Reporting,” published by the IT Governance Institute, to provide guidance on IT and financial controls. It is available as a complimentary download at www.itgi.org.

The directives of Sarbanes–Oxley require that management annually provide:

- A statement of its responsibility for establishing and maintaining adequate internal controls and procedures for financial reporting
- The conclusions about the effectiveness of the company’s internal controls and procedures for financial reporting based on management’s evaluation of those controls and procedures
- A statement that the registered public accounting firm that prepared or issued the company’s report relating to the financial statements included in the company’s annual report has attested to, and reported on, management’s evaluation of the company’s internal controls and procedures for financial reporting

“Given the significance of these directives, and the important role IT has in financial systems, many organizations have proactively enhanced the design, documentation, and consistency of IT controls,” said Zonneveld. “The work required to meet Sarbanes–Oxley requirements should not solely be regarded as a compliance process, but also as an opportunity to establish strong governance models that help ensure accountability and responsiveness to business needs.”

SARBANES–OXLEY SECTIONS 302 AND 404

The concept of a completely risk-free business environment does not exist, and will never be fully attainable. There is good news, however. In addition to the short-term improvement in controls and disclosure, the process many organizations are following to comply with Sarbanes–Oxley will have positive and lasting benefits not only for the level of investor confidence, but also for the company’s overall controls environment.

“The Sarbanes–Oxley legislation has created a greater need for businesses to have IT controls in place,” said Bill Levant, Deloitte partner and national leader for IT risk and control services. “Ensuring the reliability of financial data and maintaining ethical compliance is now the law and achieving that requires that the appropriate controls be put in place so technology can enable compliance. In addition, the opportunity to

*MANY
ORGANIZATIONS
HAVE PROACTIVELY
ENHANCED THE
DESIGN,
DOCUMENTATION,
AND CONSISTENCY
OF IT CONTROLS.*

revisit existing controls may lead to greater operating effectiveness and efficiency.”

Much of the attention, discussion, and work regarding Sarbanes–Oxley focuses on Sections 302 and 404 of the Act.

Under Section 302, chief executive officers (CEOs) and chief financial officers (CFOs) of public companies must personally certify financial statements and the existence and effective operation of disclosure controls and procedures. Every quarterly filing to the U.S. Securities and Exchange Commission (SEC) must include certification from these two executives that they have performed an evaluation of the design and effectiveness of these controls. The executives providing the certifications must also state that they have disclosed to their audit committees and independent auditors any significant control deficiencies, material weaknesses, significant changes in controls, and acts of fraud. These controls and processes help ensure that all material information is disclosed by an organization to the SEC.

Section 404 covers internal controls over financial reporting — the processes in place that are designed to ensure the reliability of the financial reporting process and, ultimately, the preparation of financial statements. This section mandates an annual evaluation of internal controls and procedures for financial reporting. As with Section 302, the CEO and CFO must personally certify the evaluation. This section also requires the company’s external auditor to independently attest to management’s assertion on the effectiveness of internal controls, including IT controls, as they relate to financial reporting.

“For many companies the increased level of engagement between IT management and external auditors under Sarbanes–Oxley will be a new challenge,” said Lynn Edelson, partner and U.S. leader for systems and process assurance at PricewaterhouseCoopers. “Senior IT management needs to start talking with the external auditors about IT controls, including documentation and testing, quarterly reviews of significant changes in the IT environment, audit committee IT oversight and fraud controls.”

The Sarbanes–Oxley requirements also have a trickle-down effect regarding certification. Some CEOs and CFOs who are required to certify their organizations’ controls are, in turn, asking the leaders of their operating units to also certify that they have implemented appropriate controls, according to *Computerworld*.

The SEC’s rules for internal control compliance with Sarbanes–Oxley are further clarified through these three objectives:

1. Records are maintained in reasonable detail to accurately and fairly reflect the transactions and dispositions of the assets of the organization.
2. There is reasonable assurance that transactions are recorded as necessary to permit preparation of financial statements in

*UNDER SECTION
302, CEOs AND
CFOs OF PUBLIC
COMPANIES MUST
PERSONALLY
CERTIFY FINANCIAL
STATEMENTS AND
THE EXISTENCE AND
EFFECTIVE
OPERATION OF
DISCLOSURE
CONTROLS AND
PROCEDURES.*

accordance with generally accepted accounting principles (GAAP), and that receipts and expenditures of the organization are being made only in accordance with authorization of management and directors of the registrant.

3. There is reasonable assurance regarding prevention of unauthorized acquisition, use, or disposition of the organization's assets that could have a material effect on the financial statements.

CONTROL FRAMEWORKS: COSO FOR FINANCIAL REPORTING AND COBIT FOR IT GOVERNANCE

Sarbanes–Oxley has also had a strong impact on corporate governance and IT governance. Previously, internal control assertions were, for the most part, voluntary and based on varying guidelines. This has changed. The Act specifically mentions *Internal Control—Integrated Framework* from the Committee of Sponsoring Organizations of the Treadway Commission (COSO) as an international control framework for financial reporting.

Internal control is defined by COSO as a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories:

- Effectiveness and efficiency of operations
- Reliability of financial reporting
- Compliance with applicable laws and regulations

Further, COSO offers the following key concepts:

- Internal control is a *process*. It is a means to an end, not an end in itself.
- Internal control is effected by *people*. It is not merely policy manuals and forms, but people at every level of an organization.
- Internal control can be expected to provide only *reasonable assurance*, not absolute assurance, to an entity's management and board.
- Internal control is geared to the achievement of *objectives* in one or more separate but overlapping categories.

Supporting the COSO framework are subsequent discussions of the Act by the Public Company Accounting Oversight Board (PCAOB), the nonprofit corporation created by the [Sarbanes–Oxley Act of 2002](#) to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports.

When COSO was first issued, there were very few IT management and control frameworks. To address this need, *Control Objectives for Information and related Technology (COBIT)*, was developed and updated by the IT Governance Institute. Over years of implementation in thousands of organizations worldwide, and with the development of *COBIT Management Guidelines*, COBIT

SARBANES-OXLEY
HAS ALSO HAD
A STRONG IMPACT
ON CORPORATE
GOVERNANCE AND
IT GOVERNANCE.

COSO SPECIFICALLY
DISCUSSES IT
CONTROL
REQUIREMENTS
IN SOME
COMPONENTS,
AND IN OTHER
COMPONENTS
REFERS TO THEM
IMPLICITLY.

has evolved into an established and globally recognized IT governance and control framework.

COSO specifically discusses IT control requirements in some components, and in other components refers to them implicitly. According to COSO, IT management is required to state that the organization has implemented a compatible IT control framework, but there is no guidance on which framework to use. According to the *IT Control Objectives for Sarbanes–Oxley* document written by Christopher Fox and Paul Zonneveld, COBIT is a rich and robust IT governance and control framework for managing risk and control of information and related technology. In the same manner that COSO identifies five components of internal control that need to be implemented to achieve financial reporting and disclosure objectives, COBIT provides similar guidance for IT.

According to COBIT, to provide the information that an organization needs to achieve its objectives, IT resources must be managed by a set of four naturally grouped processes (see [Table 1](#)).

COBIT is an open standard, has been subject to scrutiny for several years, and is the most widely used IT control framework in the world. It therefore clearly meets the SEC's requirements that control frameworks be proven and tested in the public domain. It also provides the necessary information for management to provide reasonable assurance of the IT control structure and resulting information integrity for reporting purposes to comply with Section 404 of the Sarbanes–Oxley Act.

IT GOVERNANCE AND BUSINESS STRATEGY

IT has become pervasive throughout the operations of nearly all organizations, whether they are manufacturers, not-for-profits, consultants, governmental agencies, or other entities. Boards of directors are putting the governance and control over IT on their agendas, and executives and managers are focusing increased attention on the topic.

According to an article in the *Information Systems Control Journal* by Erik Guldentops (a management consultant in Brussels, Belgium, and executive professor in the management school of the University of Antwerp), one of the main concepts incorporated into IT governance is the need to align IT with the overall business strategy. Organizations should take advantage of emerging technology to drive and execute the business strategy.

Along similar lines, Robert Kaplan (professor at Harvard Business School and chairman of the Balanced Scorecard Collaborative [BSC]), and David Norton (president of BSC), who developed the Balanced Business Scorecard process in 1990, discussed the need to map IT to business strategy in *CIO Magazine* (November 2003). According to Kaplan, different business strategies place different demands on IT resources.

Table 1 *Four Naturally Grouped Processes of IT Resources*

Plan and Organize

- Define a strategic IT plan
- Define the information architecture
- Determine the technological direction
- Define the IT organization and relationships
- Manage the IT investment
- Communicate management aims and direction
- Manage human resources
- Ensure compliance with external requirements
- Assess risks
- Manage projects
- Manage quality

Acquire and Implement

- Identify automated solutions
- Acquire and maintain application software
- Acquire and maintain technology infrastructure
- Develop and maintain procedures
- Install and accredit systems
- Manage changes

Deliver and Support

- Define and manage service levels
- Manage third-party services
- Manage performance and capacity
- Ensure continuous service
- Ensure systems security
- Identify and allocate costs
- Educate and train users
- Assist and advise customers
- Manage the configuration
- Manage problems and incidents
- Manage data
- Manage facilities
- Manage operations

Monitor and Evaluate

- Monitor the processes
- Assess internal control adequacy
- Obtain independent assurance
- Provide for independent audit

Business leaders should use a strategy map to work top-down from the organization's key value proposition offered to customers, to the critical investments in IT and human resources that will support its ability to position itself in the marketplace.

Norton noted in the *CIO Magazine* article that to accomplish this, it is critical that the IT budgeting process be integrated with the strategy of the business. One notable example is GM of Europe, where the IT group initiated the main strategy map and essentially assumed the role of consultants, building strategy maps to help define priorities of the business units.

Kaplan and Norton provide additional detail about these concepts in their recently published third book, *Strategy Maps: Converting Intangible Assets into Tangible Outcomes*.

IT HAS NOT ALWAYS
ACHIEVED THE
BOARD- AND
EXECUTIVE-LEVEL
ATTENTION IT
DESERVES.

IT GOVERNANCE ATTRACTING BOARD-LEVEL ATTENTION

Even with such renowned experts counseling the benefits of aligning IT with business strategy, IT has not always achieved the board- and executive-level attention it deserves. In a survey on the maturity of IT governance among senior officers of *Fortune* 500 entities, it was determined that six out of seven boards of directors are at least regularly informed about IT issues, two out of three boards approve IT strategy, yet only one in ten boards ask questions about IT.

This has been mostly attributed to reasons such as IT requiring more technical insight than other disciplines to understand how IT enables the enterprise, creates risks, and gives rise to new opportunities. IT also has traditionally been treated as an entity separate from the business, plus it is complex, especially in global enterprises.

Advice to boards traditionally focused on board structure, composition, size, and independence, but was short on risk management and practical IT governance. Sarbanes-Oxley requirements changed that and already have made a significant impact on board and executive attention to governance over IT.

The overall objectives of IT governance activities are to understand the issues and strategic importance of IT, ensure that the enterprise can sustain its operations, and ascertain that it can implement the strategies required to extend its activities into the future, according the *Board Briefing on IT Governance, 2nd edition*, published by the IT Governance Institute.

IT governance is the responsibility of the board of directors and executive management, although IT governance activities usually transcend management layers. IT governance is an integral part of enterprise governance and consists of the leadership and organizational structures and processes which ensure that the organization's IT sustains and extends the organization's strategies and objectives.

Boards exercising proper IT governance often uncover and address problems in advance, simply by asking the right questions, such as:

- How critical is IT to sustaining the enterprise? How critical is IT to growing the enterprise?
- How far should the enterprise go in risk mitigation, and is the cost justified by the benefit?

- Is IT a regular item on the agenda of the board, and is it addressed in a structured manner?
- Is the reporting level of the most senior IT manager commensurate with the importance of IT?

“The board of directors of my company is well aware [that] its role is to oversee the company’s organizational strategies, structures, systems, staff, and standards. However, as president of the company, it is my responsibility to ensure that they extend that oversight to the company’s IT as well,” said Michael Cangemi, president and COO, Etienne Aigner Group, Inc. “In today’s economy, and with our reliance on IT for competitive advantage, we simply cannot afford to apply to our IT anything less than the level of commitment we apply to overall governance.”

TURNING COMPLIANCE INTO COMPETITIVE ADVANTAGE

As stated previously, while Sarbanes–Oxley requirements do go a long way toward rebuilding stakeholder confidence by enhancing internal controls and timely disclosure, adhering to its principles does not completely ensure a worry-free IT environment. One way to leverage the benefits of the Act even further is to create competitive advantages that parallel the compliance process.

According to *IT Control Objectives for Sarbanes–Oxley*, building a strong internal control program within IT can help to:

- Enhance overall IT governance
- Enhance the understanding of IT among executives
- Make better business decisions with higher quality and more timely information
- Align project initiatives with business requirements
- Prevent loss of resources and the probability of system breach
- Contribute to the compliance of other regulatory requirements, such as those for privacy
- Gain competitive advantage through more efficient and effective operations
- Optimize operations with an integrated approach to security, availability, and processing integrity
- Enhance risk management competencies and prioritization of initiatives

IT GOVERNANCE CASE STUDY

One company that achieved benefits by implementing IT governance is the Charles Schwab Corporation, one of largest U.S. financial services firms engaged, through its subsidiaries, in providing securities brokerage and related financial services for more than eight million active accounts.

Charles Schwab’s diverse and complex technology environment became even more complicated after it acquired U.S. Trust and became a financial holding company. Because of the

ONE WAY TO
LEVERAGE THE
BENEFITS OF THE
ACT EVEN FURTHER
IS TO CREATE
COMPETITIVE
ADVANTAGES THAT
PARALLEL THE
COMPLIANCE
PROCESS.

THE INTERNAL
AUDIT TEAM
RECOMMENDED
COBIT.

increased regulatory oversight resulting from this acquisition, senior management sought an improved IT governance control framework.

The internal audit team recommended COBIT and mentioned that many regulatory bodies use COBIT during examinations, and therefore the framework would serve as a valuable tool to increase preparedness and facilitate communications.

Schwab implemented COBIT, which helped establish an IT governance program, maintain consistency in risk management and IS audits, ensure that its audit approach is consistent with regulatory guidelines, improve its IS control environment, enhance IT and business processes, and educate internal clients on risk and control concepts.

Schwab's approach for implementing COBIT focused on the following path:

- Map COBIT to the Federal Financial Institutions Examination Council (FFIEC) examination guidelines.* Because the Schwab Financial Holding Company must comply with banking regulations, it wanted to ensure that its audit approach was consistent with relevant regulatory examination criteria. Mapping these criteria to the COBIT domains and control objectives enabled Schwab to document its interpretation of the relationships between the COBIT domains and control objectives and the examination criteria in the *FFIEC IS Examination Handbook*, which is used by examiners to review IS operations in financial institutions.
- Map the audit universe to COBIT's high-level control objectives.* This mapping exercise ensured that each audit universe element addressed the relevant COBIT control objectives.
- Map scheduled audits to the COBIT detailed control objectives.* This became part of a mapping process completed during Schwab's yearly audit planning phase. Mapping detailed control objectives to each audit helps ensure that the strategy, objectives, and scope for each audit include all of the relevant COBIT control objectives (i.e., a completeness check to identify gaps).
- Develop a COBIT control assessment questionnaire for each audit.* These questionnaires document the results of joint risk assessments. They will be updated as processes change and reevaluated during future audits in each area. They also evaluate the effectiveness of existing processes and control mechanisms, and provide detail on risk mitigating action plans for areas that require improvements.
- Facilitate work sessions with clients.* Proactive projects have had a positive impact on client relationships and have helped ensure consistency in the application of risk assessments over IT functions. They help evaluate the effectiveness of controls in place for the area under review. To ensure consistency and collaboration, the assessment results are documented using COBIT maturity ratings highlighted in the *COBIT Management Guidelines* component.
- Analyze, document, and validate results.* Schwab evaluated results of the joint risk assessment process by executing its audit work programs and performing tests of controls. It used the *COBIT Audit Guidelines* to facilitate audit testing, where relevant, by comparing existing audit work programs to the *COBIT Audit*

Guidelines framework. After the testing is complete, results of each audit are documented in an audit report issued to senior management.

Implementing COBIT as part of its audit process has significantly enhanced Schwab's risk assessment process and has provided a confidence that its audit strategy covers industry best practices and control objectives. U.S. Federal Reserve Board examiners have confirmed that Schwab's implementation of a COBIT-based audit approach is an appropriate method for assessing IT risks. Other benefits include increased client participation in audits and positive impacts on relationships with clients. Involved parties now believe internal audit's approach is effective and a beneficial situation for all stakeholders.

ORGANIZATIONS RESPONDING TO IT SECURITY ISSUES

Threats and weaknesses will always exist for the key information that is recorded on, processed by, stored in, shared by, transmitted, or retrieved from electronic media. Information and information technology must be protected against harm from vulnerabilities such as loss, inaccessibility, alteration, and wrongful disclosure, whether they are caused by errors and omissions, fraud, accidents, or intentional damage.

Too often, information security has been dealt with solely as a technology issue, with little consideration given to enterprise priorities and requirements. Instead of treating information security as a separate issue, it should be addressed in every phase of a project.

According to *Information Security Governance: Guidance for Boards of Directors and Executive Management*, published by the IT Governance Institute, boards and management have several fundamental responsibilities relative to information security governance, including:

- Understand why information security needs to be governed.
- Ensure it fits in the IT governance framework.
- Take board-level action.
- Take management-level action.

"The most important thing a CIO can do to make his or her business safer is clearly articulate an IT security policy, make sure everyone in the organization knows their piece of it, and then enforce it," said Richard Clarke, former White House advisor for cyberspace security, in *CIO Insight* magazine. "You can't assume anymore that your system is going to be infallible. And if you throw all of your money into one thing and don't sit back first and define an IT security policy, then you'll probably end up spending your money foolishly."

A study from the Council on Competitiveness shows that companies are increasingly paying attention to security concerns, with 83 percent of companies having conducted risk

TOO OFTEN,
INFORMATION
SECURITY HAS
BEEN DEALT WITH
SOLELY AS A
TECHNOLOGY
ISSUE.

IT FAILURES DO
AFFECT THE IMAGE
AND REPUTATION IN
OUR INCREASINGLY
INTERCONNECTED
ECONOMY.

assessments in 2003, compared to only 34 percent in 2002. In addition, companies reported taking a much closer review of critical infrastructure — a key concern of the Department of Homeland Security. In 2002, less than 40 percent of companies reported risk assessments in electronic communications, electrical power connections, or telecommunications. A year later, 71 percent said they conducted comprehensive assessments of electronic communications, 68 percent of financial assets, and 58 percent of telecommunications and electric power connections.

MOVING FORWARD

IT is now permanently interwoven with all aspects of business. As the impact of the Sarbanes–Oxley Act and similar legislation continues to dramatically change the way organizations approach internal control, disclosure, and overall responsibility, IT governance will continue to mature.

Erik Guldentops in the *Information Systems Control Journal* noted that “There is no denying that an efficient and effective information infrastructure does affect shareholder value. What is more, IT failures do affect the image and reputation in our increasingly interconnected economy. It will be interesting to see how IT will be positioned in the regulatory requirements for internal control and governance.”

Management is always searching for condensed and timely information to make informed decisions on difficult issues such as IT risk and control. The first step, according to the *COBIT Management Guidelines*, is for every organization to understand the status of its own IT systems and to decide what security and control it should provide. Obtaining an objective view and creating a business case for expenditure to improve control and security are not easy tasks. The management guidelines respond to this need and address the following management concerns:

- Performance measurement*: What are the indicators of good performance?
- IT control profiling*: What is important? What are the critical success factors for control?
- Awareness*: What are the risks of not achieving our objectives?
- Benchmarking*: What do others do? How do we measure and compare?

To help focus on performance management, the principles of the balanced business scorecard were used to assist in defining key goal indicators and key performance indicators.

In this era of omnipresent technology, all organizations need to demonstrate appropriate levels of internal control and security. Every entity must take the appropriate steps to understand its own performance and measure its progress. This is a challenging and ongoing process, but it benefits all stakeholders.

Organizations must continually work toward satisfying the quality, fiduciary, and security requirements for their information, as they do for all assets. This is a constantly changing goal, as management must demonstrably attain increasing levels of security and control. While most enterprises recognize the benefits that new technology can offer, successful organizations will focus on understanding and managing the associated risks. ■

Marios Damianides, CISM, CISA, CPA, CA, is a partner, Technology and Security Risk Services (TSRS), Ernst & Young, New York City. He has more than 20 years of experience in information systems, with a focus on security and enterprise systems management. He has assisted in designing and implementing systems management and security architecture solutions for numerous Fortune 100 companies. A member of ISACA since 1992, Damianides was elected international president in July 2003, and also serves as international president of the IT Governance Institute. Damianides has written many business and technical articles and has presented papers at several prestigious conferences.

IT Governance Checklist

Questions to Ask to Uncover IT Issues

	V	A	R	P
Is it clear what IT is doing?		✓		
How often do IT projects fail to deliver what they promised?	✓	✓		
Are end users satisfied with the quality of the IT service?	✓			
Are sufficient IT resources and infrastructure available to meet required enterprise strategic objectives?	✓	✓		
Are IT core competencies maintained at a sufficient level to meet required enterprise strategic objectives?	✓	✓		
How well are IT outsourcing agreements being managed?	✓		✓	✓
What has been the average overrun of IT operational budgets?				✓
How often and how much do IT projects go over budget?				✓
How long does it take to make major IT decisions?		✓	✓	
Are the total IT effort and investments transparent?	✓			✓
How much of the IT effort goes to firefighting rather than enabling business improvements?	✓	✓		
Is the enterprise's internal IT skill set decreasing, and how successfully are skilled IT resources attracted to the organization?		✓	✓	
How well do the enterprise and IT align their objectives?		✓		

Questions to Ask to Find Out How Management Addresses the IT Issues

	V	A	R	P
How critical is IT to sustaining the enterprise? How critical is IT to growing the enterprise?	✓	✓	✓	
What strategic initiatives has executive management taken to manage IT's criticality relative to maintenance and growth of the enterprise, and are they appropriate?		✓		
What is the organization doing about leveraging its knowledge to increase shareholder value?	✓			
What IT assets are there, and how are they managed?			✓	✓
Are suitable IT resources, infrastructures, and skills available to meet the required enterprise strategic objectives?		✓		
Is the enterprise clear on its position relative to technology: pioneer, early adopter, follower, or laggard?	✓	✓		

Questions to Ask to Find Out How Management Addresses the IT Issues (continued)	V	A	R	P
Is IT participating in overall corporate change setting and strategic direction? Do IT practices and IT culture support and encourage change within the enterprise?		✓		
Do the enterprise research technology, process, and business prospects set the direction for future growth?		✓		
Are enterprise and IT objectives linked and synchronized?		✓		
Is the enterprise clear on its position relative to risk: risk avoidance or risk taking?			✓	
Is there an up-to-date inventory of IT risks relevant to the enterprise?			✓	
What has been done to address these risks?			✓	
How far should the enterprise go in risk mitigation, and is the cost justified by the benefit?			✓	
What are other organizations doing, and how is the enterprise placed in relation to them?		✓		✓
What is industry best practice, and how does the enterprise compare?	✓			✓
What is management doing to address risks?		✓		
Is the board regularly briefed on risks to which the enterprise is exposed?			✓	
Based on these questions, can the enterprise be said to be taking "reasonable" precautions relative to technology risks?		✓	✓	

Questions to Ask to Self-Assess IT Governance Practices	V	A	R	P
How certain is the board about the answers provided to the above questions?				✓
Is the board aware of the latest developments in IT from a business perspective?		✓		
Is IT a regular item on the agenda of the board, and is it addressed in a structured manner?		✓		
Does the board articulate and communicate the business direction to which IT should be aligned?		✓		
Is the board aware of potential conflicts between the enterprise divisions and the IT function?		✓	✓	
Does the board have a view on how and how much the enterprise invests in IT compared to its competitors?	✓			✓
Is the reporting level of the most senior IT manager commensurate with the importance of IT?		✓		
Does the board have a clear view on the major IT investments from a risk and return perspective?	✓		✓	
Does the board obtain regular progress reports on major IT projects?	✓			✓
Does the board obtain IT performance reports illustrating the value of IT from a business driver's perspective (customer service, cost, agility, quality, etc.)?	✓			✓
Is the board regularly briefed on IT risks to which the enterprise is exposed, including compliance risks?			✓	
Is the board assured of the fact that suitable IT resources, infrastructures, and skills are available (including external resourcing) to meet the required enterprise strategic objectives?		✓		
Is the board getting independent assurance on the achievement of IT objectives and the containment of IT risks?	✓		✓	✓

Note: **V** = IT Value Delivery; **A** = IT Strategic Alignment; **R** = Risk Management; **P** = Performance.