

IT Governance: Why a Guideline?

By Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP

Introduction

IT governance is the responsibility of the board of directors and executive management. It is an integral part of enterprise governance and consists of the leadership and organizational structures and processes to ensure that the organization's IT sustains and extends its strategies and objectives.

This definition, which comes from the IT Governance Institute® portal at www.itgovernance.org, explains the difficulties of establishing an effective information technology (IT) controls framework within an organization. Many variables should be considered, from human behavior and organizational environment to complex technical aspects.

IT governance is the responsibility of executives and is not an isolated discipline or activity, but rather is integral to enterprise management. The purpose of IT governance is to direct IT endeavors to ensure that IT's performance meets the objectives so that:

- IT's alignment with the enterprise results in the promised benefits being realized.
- IT enables the enterprise so that opportunities are exploited and benefits are maximized.
- IT resources are used responsibly.
- IT-related risks are managed appropriately.

The objectives of IT governance activities are to understand the issues and the strategic importance of IT, to ensure that the enterprise can sustain its operations and to ascertain that it can implement the strategies required to extend its activities into the future. IT governance practices aim to ensure that expectations for IT are met and IT risks are mitigated.

IS Auditing Standards

The specialized nature of information systems (IS) auditing, and the skills necessary to perform such audits, require standards that apply specifically to IS auditing. One of the goals of Information Systems Audit and Control Association (ISACA) is to advance globally applicable standards to meet this need. Standards define mandatory requirements for IS auditing and reporting.

Guidelines also have been developed to provide guidance in applying ISACA IS Auditing Standards. The IS auditor should consider them in determining how to achieve implementation of the standards, use professional judgment in their application and be prepared to justify any departure.

The guideline on IT Governance was created to provide guidance on the IS Auditing Standard 060 Performance of Audit Work, section 060.020 Evidence, which states: "During the course of the audit, the information systems auditor is to

obtain sufficient, reliable, relevant and useful evidence to achieve the audit objectives effectively. The audit findings and conclusions are to be supported by appropriate analysis and interpretation of this evidence."

The Need for a Guideline

The COBIT *Executive Summary* states: "Organisations must satisfy the quality, fiduciary and security requirements for their information, as for all assets. Management also must optimise the use of available resources including data, application systems, technology, facilities and people. To discharge these responsibilities, as well as to achieve its objectives, management must establish an adequate system of internal control."

The use of technology in all aspects of economic and social endeavors has created a critical dependency on IT to initiate, record, move and manage all aspects of economic transactions, information and knowledge, creating a critical place for IT governance within enterprise governance.

High-profile problems (e.g., system failures resulting from virus attacks, loss of trust or systems availability due to web site hacking) experienced by a variety of public and private sector organizations have focused attention on enterprise governance issues. The formal means by which management discharges its responsibility to establish an effective system of internal control over an organization's operational and financial activities can be subject to public scrutiny and often forms part of the audit scope for internal and external IS auditors.

The Guideline on IT Governance

The purpose of the *IT Governance* guideline is to provide information on how an IS auditor should approach an audit of IT governance. It covers the appropriate organizational position of the IS auditor concerned, issues to consider when planning the audit, and evidence to review when performing the audit. This guideline also provides guidance on reporting lines and content and the follow-up work to be considered. The IT Governance guideline is divided into six sections:

1. **Audit charter**—IT governance, as one of the pillars of enterprise governance, comprises the body of issues addressed in considering how IT is applied within the enterprise. IT is now intrinsic and pervasive within enterprises, rather than being a separate function marginalized from the rest of the enterprise. How IT is applied within the enterprise will have an immense effect on whether the enterprise will attain its mission, vision or strategic goals. For this reason, an enterprise needs to evaluate its IT governance, as it is becoming an increasingly important part of the overall enterprise governance. Reporting on IT governance involves auditing at the highest level in the organization and may cross

divisional, functional or departmental boundaries. The IS auditor should confirm that the terms of reference state the:

- Scope of work, including a clear definition of the functional areas and issues to be covered
- Reporting line to be used where IT governance issues are identified to the highest level of the organization
- Auditor's right of access to information

2. **Independence**—The IS auditor should consider whether his/her organizational status is appropriate for the nature of the planned audit. Where this is not considered to be the case, the appropriate level of management should consider hiring an independent third party to manage or perform this audit.

3. **Planning**—This section focuses on the information gathering and planning for the audit phases. The IS auditor is recommended to obtain information on the IT governance structure, including the levels responsible for governing the enterprise and setting the enterprise's strategic directions. The skills and IT infrastructure required to meet the strategic goals set for the enterprise need to be assessed. Finally, the enterprise's capability to sustain its current level of operations must be assessed.

The IS auditor should identify and obtain a general understanding of the processes that enable the IT governance structure to perform its functions in an adequate manner, including the communication channels used to set goals and objectives to lower levels (top-down) and the information used to monitor its compliance (bottom-up).

The IS auditor should obtain information on the organization's IS strategy (whether documented or not), such as:

- Long- and short-range plans to fulfill the organization's mission and goals
- Long- and short-range strategy and plans for IT and systems to support those plans
- An approach to setting IT strategy, developing plans and monitoring progress against those plans
- An approach to change control of IT strategy and plans
- An IT mission statement and agreed goals and objectives for IT activities
- Assessments of existing IT activities and systems

The detailed objectives for an IS audit of IT governance ordinarily will depend upon the framework of internal control exercised by top-level management. In the absence of any established framework, the *COBIT Framework* should be used as a minimum basis for setting the detailed objectives. The IS auditor should include in the scope of the audit the relevant processes for planning and organizing the IT activity and the processes for monitoring that activity. The scope of the audit should include control systems for the use and protection of the full range of IT resources defined in the *COBIT Framework*.

4. **Performance of audit work**—IT governance, as part of enterprise governance, should be driven by business goals and objectives. The IS auditor should evaluate whether there is a business strategic planning process in place by considering various aspects, such as whether there is a clear definition of business vision and mission.

The guideline specifies the differences among different

audit goals: reviewing the IT strategic planning process, the IT tactical planning and the delivery process. Finally, special consideration is given to the application development methodology and practices, and the controls applied over the development process. The review of the processes used to administer the current systems portfolio also is covered, where the IS auditor should consider the coverage of organizational strategic and support areas by the current systems. The IS auditor should consider whether top-level management has initiated the appropriate management activities in relation to IT, and whether those activities are being monitored appropriately.

In reviewing the processes used to administer the current systems portfolio, the IS auditor should consider the coverage of organizational strategic and support areas by the current systems. The IS auditor may include in the review the overall coverage of the policies issued, providing the strategic areas defined by the business strategic planning process. The process followed by top-level management to elaborate, communicate, enforce and monitor policy compliance may be reviewed. It may be appropriate to review documented policies on security, human resources, data ownership, end-user computing, intellectual property, data retention, system acquisition and implementation, outsourcing, independent assurance, continuity planning, insurance and privacy.

Assessing whether the definition of roles and responsibilities of the people involved in the processes is appropriate to support the processes involved in the review and whether they have the skills, experience and resources needed to fulfill their roles should be considered.

Whether the appropriate level of involvement of internal audit has been provided should be determined. An assessment should be completed to determine whether the position of IT specialist staff is appropriate for the organization to make the best use of IT to achieve its business objectives and whether the position is adequate to address the risks to the organization of errors, omissions, irregularities or illegal acts.

The IS auditor should consider whether the audit evidence obtained from the previously mentioned reviews indicates coverage of the appropriate areas. Information that should be considered includes the IT mission statement and agreed goals and objectives for IT activities, IT strategy plans to implement the strategy and monitoring of progress against those plans, IT budgets and monitoring of variances. An assessment should be made of the risks associated with the organization's use of IT resources; the approach to managing those risks; and the high-level policies for IT use, protection and monitoring of compliance with those policies. A comparison should be made of relevant performance indicators for IT, such as benchmarks from similar organizations, functions, appropriate international standards, maturity models or recognized best practices, and the performance-against-agreed performance indicators should be regularly monitored. IS audit evidence should be obtained from the periodic reviews of IT by the governance function. Action items should be identified, assigned, resolved and tracked, and effective and meaningful links among the processes should be obtained from reviews.

Additionally, the IS auditor should consider whether top-level management has initiated the appropriate management activities in relation to IT, and whether those activities are being appropriately monitored.

5. **Reporting**—The IS auditor should address reports on IT governance to the audit committee and top-level management. When inadequacies in IT governance are identified, they should be reported immediately to the appropriate individual or group defined in the audit charter or engagement letter. In addition to compliance with other ISACA guidance on reporting, some of the contents of the audit report on IT governance might include:

- A statement that top-level management is responsible for the organization's system of internal control
- A statement that a system of internal control can provide only reasonable, and not absolute, assurance against material misstatement or loss
- A description, and the related supporting documentation, of the key procedures that top-level management has established to provide an effective IT governance system
- Information pertaining to any noncompliance with the organization's policies or any relevant laws and regulations or industry codes of practice for enterprise governance
- Information on any major uncontrolled risks
- Information on any ineffective or inefficient control structures, controls or procedures, along with the IS auditor's recommendations for improvement
- The IS auditor's overall conclusion on the enterprise's IT governance, as defined in the terms of reference

6. **Follow-up activities**—The effects of any weaknesses in the system of enterprise governance ordinarily are wide-ranging and high risk. Therefore, the IS auditor should carry out sufficient, timely follow-up work to verify that management action to address weaknesses is taken promptly.

Conclusions

IT governance, as part of enterprise governance, should be driven by business goals and objectives. The IS auditor should evaluate whether there is a business strategic planning process in place by considering various aspects, such as whether there is a clear definition of business vision and mission. The guideline then specifies the differences among audit goals, reviewing the IT strategic planning, IT tactical planning and the delivery process. Finally, special consideration is given to the application development methodology and practices, and the controls applied over the development process. The review of the processes used to administer the current systems portfolio also is covered, i.e., where the IS auditor should consider the coverage of organizational strategic and support areas by the current systems.

Editor's note:

The ISACA Standards Board has an ongoing development program and welcomes the input of ISACA members and other interested parties to identify emerging issues requiring new standards. Refer to www.isaca.org/standard/stdownload.htm for the complete set of guidance. Any suggestions should be e-mailed to research@isaca.org, faxed to +1.847.253.1443 or mailed to the ISACA International Headquarters at 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008, USA, to the attention of the ISACA standards department.

Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP

is a professional information security consultant. He is responsible for many IS audit projects at KPMG. He has consulted for many major companies in the IT field, including electronic and IS technologies, both for civil and military sectors; information systems for production, software quality, security of the information systems and installations. He is the chair of the ISACA Standards Board as well as a frequent speaker at many international conferences and seminars.

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 2003 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