IT Governance: IT Audit Role

By Frederick Gallegos, CISA, CDE, CGFM, MSBA

IT governance begins when an organization realizes that it is a part of a larger commerce picture. The Global Information Infrastructure (GII), still in the early stages of its development, already is transforming our world. The US Department of Homeland Security's (DHS) recently released plan, "The National Strategy for Securing Cyberspace," is an effort to integrate IT security and control into our lives. Over the next decade, advances on the GII will affect almost every aspect of daily life—education, health care, work and leisure activities. Disparate populations, once separated by distance and time, will experience these changes as part of a global community.

No single force embodies our electronic transformation more than the evolving medium known as the Internet. Once a tool reserved for scientific and academic exchange, the Internet has emerged as an appliance of everyday life, accessible from almost every point on the planet. Students globally are discovering vast treasure troves of data via the World Wide Web. Doctors are utilizing telemedicine to administer offsite diagnoses to patients in need. Citizens of various nations are finding additional outlets for personal and political expression. The Internet shows how to reinvent government and reshape our lives and our communities through IT.

As IT empowers citizens and democratizes societies, it also is changing classic business and economic paradigms. New models of commercial interaction are developing as businesses and consumers participate in the electronic marketplace and reap the beneficial results. Entrepreneurs are able to start new businesses more easily, with smaller upfront investment requirements, by accessing the Internet's worldwide network of customers.

GII is a global analysis of information storage, transmission, interoperability and applications for the information superhighway. It begins with high-speed networks, delivery systems, LANs and interfacing, and progresses to storage and server capabilities, and then examines the home, business, education and medical applications of these technologies. Wireless networks and fiber-optic technology also are explored, their continuing integration being a pivotal factor in defining the information infrastructure. As individual standalone computer systems have been incorporated into an ever larger network (e.g., local area networks, wide area networks, Internet, etc.), the requirement for global information infrastructure also has increased. Today, users of computer systems can be connected with one another worldwide through the public switched telecommunications network, satellites, microwave towers and radio transmitters. Thus, it is imperative for users and systems to identify themselves to one another with a high degree of certainty and for distant systems to know with assurance what privileges for accessing databases or software processes are gained via remote request. Protection that once could be obtained by geographic propinquity and personal recognition of users must now be provided electronically and with extremely high levels of certainty. Again, within the DHS proposal is the "National Strategy for the Physical Protection of Critical Infrastructures and Key Assets." This strategy will set the foundation for corporate and government information infrastructures.

The Corporate Information Infrastructure

The corporate information infrastructure and electronic government information infrastructure must coexist with the national information infrastructure, which is driven by the GII. IT governance can allow the organization to come to terms with this issue as it reorganizes for the next level of competition—the global market. The obstacles management may face when implementing a companywide reorganization could be few or many, depending on the thoroughness of the diagnosis, design, implementation and monitoring of the reorganization. As a result of the US initiatives, more than 300 CEOs have formed a task force (*www.technet.org*) to help develop a strategy for securing cyberspace within the corporate information infrastructure.

Management should expect to encounter various reactions to its reorganization from internal sources—its employees—first. Employees react to change differently and some reactions can have a profound impact on the success of an organization. Some employees will accept, support and welcome the changes; however, others will not. Dissatisfaction can result and valuable employees may leave the company. Employees need to feel valued, be given adequate tools and knowledge to contribute, and be adequately compensated for that contribution. Careful thought must be given to alleviate or decrease the impacts on employee morale and dissatisfaction to protect the organization.

IT Audit's Role and Management Role

The IT auditor and IT management must review existing standards and ensure compliance with national information infrastructures. If they compete beyond the national boundary, then they must ensure that they are compliant with GII. This may be a way of minimizing damage from internationally developed and disseminated computer viruses, such as the "ILOVEYOU" virus. The national, electronic government and corporate information infrastructures can become barriers to such nuisances if they complement each other and place importance on risk.

Risk in these areas must be reviewed continuously to ensure compliance, compatibility and security. System security for such infrastructures requires planning, implementation and continuous monitoring. Government has taken the lead in this area, especially the US federal government. In essence, it has moved into an electronic government era.

The auditor evaluating today's complex systems must have highly developed technical skills to understand the evolving methods of information processing. Contemporary systems carry such risks as noncompatible platforms, new methods to penetrate security through communication networks (e.g., the Internet), and the rapid decentralization of information processing with the resulting loss of centralized controls.

Auditing the processing environment is divided into two parts. The first and most technical part of the audit is the evaluation of the operating environment, with major software packages (e.g., the operating and security systems) representing the general or environmental controls in the automated processing environment. This part usually is audited by the IS audit specialist. The second part of the processing environment is the automated application, which is audited by the general auditor who possesses some computer skills.

As the use of IT within organizations continues to grow, auditing computerized systems must be accomplished without many of the guidelines established for the traditional auditing effort. In addition, new uses of IT introduce new risks, which in turn require new controls. IS auditors also are in a unique position to evaluate the relevance of a particular system to the enterprise as a whole. Because of this, the IS auditor often plays a role in senior management decision-making.

The role of IS auditor can be examined through the process of IT governance and the existing standards of professional practice for this profession. As previously mentioned, IT governance is an organizational involvement in the management and review of the use of IT in attaining the goals and objectives set by the organization.

Since IT impacts the operation of an entire organization, everyone should have an interest and role in governing its use as well as the application of this valued resource. The growing awareness has led many organizations to recognize that if they are to make the most of their IT investment, and protect that investment, they need a formal process to govern it.

Reasons for implementing an IT governance program include:

- Increasing dependence on information and the systems that deliver the information
- Increasing vulnerabilities and a wide spectrum of threats
- Scale and cost of current and future investments in information and information systems
- Potential for technologies to dramatically change organizations and business practices, create new opportunities and reduce costs

As long as these factors remain a part of business, there will be a need for effective, interdependent systems of enterprise and IT governance. IT auditors have an important role in this process.

An open standard IT governance tool that helps nontechnical and technical managers and auditors understand and manage risks associated with information and related IT was developed by the IT Governance Institute. *Control Objectives for Information and related Technology* (COBIT) is a comprehensive framework of control objectives designed to help IS auditors, managers and executives discharge fiduciary responsibilities, understand their IT systems and decide what level of security and control is adequate. COBIT provides an authoritative, international set of generally accepted IT practices for business managers and auditors.

COBIT can be downloaded on a complimentary basis from *www.isaca.org*. It includes a publication containing detailed management guidelines to bridge the gaps among business risks, control needs and technical issues. These new tools help businesses monitor processes by using critical success factors (CSFs), key goal indicators (KGIs), key performance indicators (KPIs) and maturity models (MMs). Additional resources and information are available at *www.itgi.org*.

References

CEO Task Force for Securing Cyberspace, *www.technet.org*

The National Strategy for Securing Cyberspace, *www.whitehouse.gov/pcipb*

National Strategy for the Physical Protection of Critical Infrastructures and Key Assets, *www.whitehouse.gov/pcipb/physical.html*

Gallegos, Frederick; Dan Manson; Sandra Senft; *Information Technology Control and Audit*, Auerbach /CRC Press, June 1999

Gallegos, Frederick; "Auditing Global Information Infrastructure and National Information Infrastructure," EDP Auditing Series, Auerbach/CRC Press, January 2000, pp. 1-16

Gallegos, Frederick; Jae Up Kim; "Policy of GII (Global Information Infrastructure) and Security Control Auditing of NII (National Information Infrastructure) and Electronic Government (EG)"

Frederick Gallegos, CISA, CDE, CGFM, MSBA
is audit advisor and faculty member of the Computer Information Systems Department of California State Polytechnic University, Pomona. He has more than 30 years of industry experience in the information systems audit, security and control field. He has more than 30 years of teaching experience in this field at the academic and professional level. In addition, he has published five books and more than 200 articles in the information audit, control and security field.

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*.