ITGI: IT Governance Institute

Mollie E. Krehnke

Abstract
The perspectives and actions of information technology (IT) professionals, information security professionals, and auditors will impact the IT stance of an organization and the ability of IT to securely and consistently meet and exceed the objectives of an enterprise in a global community. The IT Governance Institute has become a strategic force and a leading reference on IT-enabled business systems governance for the global business community.

PURPOSE
Federal regulations, business competition, complex information and communication technologies, and expanded worldwide connectivity increase the risks associated with doing business. The information technology Governance Institute (ITGI) was established to:

- Raise awareness and understanding of enterprise business and technology risks
- Provide guidance and tools to those responsible for IT at all levels
- Enable those professionals to conduct their responsibilities in such a manner that IT meets and exceeds internal (business) and external (federal) requirements
- Empower those professionals in the mitigation of their business process-related risks through the provision of pertinent publications based on extensive, focused, applied (as opposed to basic) research.[1]

HUMBLE BEGINNINGS
The ITGI was established by the Information Systems Audit and Control Association (ISACA) in 1976 as the Information Systems Audit and Control Foundation.[1] ISACA was formed in 1967 and incorporated in 1969 as the Electronic Data Processing Auditors Association by a group of professionals who audited controls in the computer systems in their respective companies. In 2003, the ITGI was established to undertake large-scale research efforts to expand the knowledge and value of the IT governance and control field.

The new name reflects the expanded role of IT in the support of business enterprises—the enablement and transformation—of enterprise growth and (even) survival, and further embraces the many disciplines that are responsible for IT governance within the business enterprises such as audit, assurance, information security, control, and privacy.

OPERATIONS AND FUNDING
ITGI accomplishes its objective as a 501(c)3 not-for-profit and vendor-neutral organization. Volunteers use their personal time to create, review, and publish the deliverables that are made available under the ITGI cognizance. No Information ISACA member dues are used to support the activities of ITGI. Personal and corporate contributions can be made to ITGI to offset the institute costs, and gifts of over U.S. $25 are acknowledged as a contribution in the ISACA/ITGI annual report.[1] The various opportunities for contributions (affiliates, sponsors, and donors) are described on the ITGI website.

RESEARCH FOCUS AND ASSOCIATED DELIVERABLES
The research conducted by ITGI “contributes to a new level of excellence in practices worldwide, by evaluating and analyzing emerging guidelines for implementation and control of new technologies and applications, capitalizing on technological advances to help enterprises achieve competitive advantage, bringing a global perspective to the critical issues facing senior management, and providing practitioners a specialized viewpoint.”[1]

The ITGI “strives to assist enterprise leadership in ensuring long-term, sustainable enterprise success and increased stakeholder value by expanding awareness of the need for and benefits of effective IT governance. The institute develops and advances understanding of the vital link between IT and enterprise governance, and offers best practice guidance on the management of IT-related risks”.[2]
By conducting original research on IT governance and related topics, ITGI helps enterprise leaders understand the relationship of IT to business objectives and have the tools to ensure effective governance over IT within their enterprises. The resource center on the ITGI website includes articles, white papers, slide presentations, survey results, links, and other resources. Many publications are available in downloadable form, and hard copies are available from the ISACA bookstore. The major categories for the ITGI research are:

- Security control and assurance
- Accounting, finance, and economics
- Business, management, and governance
- Contingency planning and disaster recovery
- IT
- Risk management

ISACA members are granted a discount on the publications (generally $10–100 per item) that, over time, can result in substantial savings to an individual or an organization. Academic and bulk discounts are also available to those who qualify. ISACA journals have a section in the back entitled The ISACA Bookstore that lists new products and a description of those products and a bookstore price list for several hundred deliverables. The website provides a complete description for all deliverables at http://www.isaca.org/bookstore.

The content and scope of ITGI deliverables is continually expanding, and past research is enhanced to reflect new regulations, technologies, and changed business processes. An example of this would be the newest Control Objectives for Information and related Technology (COBIT) 4. (Trademark registered by ISACA.) This version “emphasizes regulatory compliance, helps organizations to increase the value attained from IT, and enables and simplifies implementation of the COBIT Framework.”

USING ITGI PRODUCTS TO GUIDE AND SUPPORT INITIATIVES

The number of ITGI products continues to expand, and the focus of many research deliverables is international in scope (and in language, including Japanese, German, and French). For example, a deliverable from the COBIT Mapping research project is COBIT Mapping: Overview of International IT Guidance that focuses on the business drivers for implementing international IT guidance documents and the risks of non-compliance. Another available resource is A Guide to Cross-Border Privacy Impact Assessment that addresses principles and questions associated with the collection, use, and disclosure of personally identifiable information that may be subject to regulation. The ITGI landmark study in 2003 and follow up survey in 2005 present IT governance perceptions and activities worldwide, as noted by senior IT executives and enterprise executives, entitled the IT Governance Global Status Report.

The best way to learn what is available is to routinely visit the ITGI and ISACA web sites. However, some product reviews are listed below to present a more detailed sampling of the offerings. ITGI makes excerpts available for review, so the reader can make a determination as to the usefulness of a product before purchasing it.

Members of the ISACA can read the book reviews in the Information Systems Control Journal to see if a particular product would be beneficial to their work. Examples of reviews of ITGI products are summarized below.

Information Security Governance

The Information Security Governance: Guidance for Boards of Directors and Executive Management document presents a big punch in a small package. The document defines management-level actions that ensure information security addresses the IT structure and the needs of the business and presents questions for directors and management, best practices, and critical success factors to facilitate the deployment of the desired actions. The document also provides an information security governance maturity model that can be used to define an organization’s security ranking. The ranking can then be used as the focal point for determining subsequent strategies for the improvement of the security of the organization.

International Information Governance Practices

Strategies for IT Governance is a collection of research articles on IT governance written by academics and practitioners from different countries with a message of IT governance as a business imperative and a top management priority. The book presents case studies that show how IT governance can work in practice. In addition, COBIT is considered to be a valuable resource in many countries as an organizational standard or guideline for multiple topics, including IT management, IT governance, and auditing. This is well presented in the text and figures in the article, “The Value to IT of Using International Standards,” by Ernst Jan Oud. The article also discusses the value associated with the implementation of a de facto standard, or set of best practices, rather than developing standards from scratch; although, the need for customizing the practices to meet company objectives is strongly emphasized.
Network Security for Business Processes Governed by Federal Regulations

Network Security: The Complete Reference presents a broad spectrum of security topics, including return on security investment; security strategy and risk analysis; security policy development and security organizations; access control and physical security; biometrics; e-mail; network architecture; firewalls and Intrusion Detection Systems; Virtual Private Network; wireless security; disaster recovery; Windows, Linux, UNIX, and Novell; application and database security; and incident response. The book will be useful to security professionals, IT administrators, and software developers who are writing secure code for the J2EE and .NET platforms.[8]

Secure Outsourcing of IT Functions

Outsourcing Information Security by C. Warren Axelrod is a risk-based approach to outsourcing according to the reviewer, Sarathy Emani, an IT professional with international experience. The book “explains the issues one needs to identify, quantify, and analyze to make the right outsourcing decisions without sacrificing security.” Topics included in the book are, the history of IT outsourcing, internal and external security risks associated with outsourcing, motivations and justifications behind outsourcing, objectives of outsourcing, tangible and intangible costs and benefits, the outsourcing evaluation and decision process, and candidate security services for outsourcing. The book will be useful to managers, information security, and IT senior management professionals who are directly involved in outsourcing or business partner relationships.[9]

Business Impacts for an Unavailable e-Commerce Service

The e-Commerce Security series, particularly e-Commerce Security—Business Continuity Planning, provides guidance to businesses and organizations in the creation of a plan to reduce the risk associated with such an event and to recover more quickly if resources are unavailable. The book addresses:

- Business continuity planning and evaluation
- Business assessment
- Strategy selection
- Plan development
- Testing and maintenance.

According to Linda Kinczkowski, it will be useful to business managers, security and audit professionals, and educators and students who have to address business continuity and disaster planning. The book also presents precautions and procedures that apply specifically to the e-commerce business component.[10]

Financial Audit Processes

Auditing: A Risk Analysis Approach, Fifth Edition, “offers an in-depth framework that addresses the relationships among audit evidence, materiality, audit risk and their concrete applications.” In addition, the book provides resources that would be useful for anyone studying for the Certified Public Accountant (CPA) and Certified Internal Auditor exams based on the review questions and essays provided at the end of each entry and the computer audit practice case. Students, accountants, chief financial officers (CFOs), CPAs, IT auditors, and faculty members teaching financial audit will find this to be a useful resource.[11]

Internal Audit Processes

The book, Managing the Audit Function: A Corporate Audit Department Procedures Guide, Third Edition, is very comprehensive, addressing all aspects of the internal auditing function. The procedural format provides a resource that could be used as a starting point for many organizations and includes audit plans, work papers, and descriptions of the roles and responsibilities for the audit team. The third edition, with its expanded focus on internal auditing, is applicable for internal audit managers and management for large and small businesses. The book also includes a discussion of other factors that impact corporate business processes, including the United States’ Sarbanes–Oxley Act of 2002 and the Foreign Corrupt Practices Act. The reviewers felt that this book is an essential resource for every audit department.[12]

Risk-Based Auditing Processes

Auditor’s Risk Management Guide—Integrating Auditing and Enterprise Risk Management (ERM) is a guide for conducting a risk management-based auditing methodology and provides case studies that utilize the concepts presented. Topics include an overview of ERM; control-based, process-based, risk-based, and risk management-based auditing approaches; an integration of strategy into risk management-based auditing; and risk assessment quantification techniques. The book also includes a CD-ROM containing electronic versions of work programs, checklists, and other tools. The reviewer felt that this book is "outstanding in the way it is organized and the extent of details it covers and the presentation from generalities to specifics aids the reader in understanding the concepts being presented."[13]
Oracle® Database Security, Privacy, and Auditing Requirements

Oracle Security Privacy Auditing addresses HIPAA technical requirements but is also an excellent primer on Oracle database security, describing what is arguably best practice, which is why it is assessed as valuable even to a reader who is not specifically concerned with Health Insurance Portability and Accountability Act.” The authors are distinguished Oracle professionals, and the presentation enables the reader to skim through the text and read only the portions that are pertinent for a particular concern. However, the book is addressed to database administrators, architects, system developers, and designers, and the reader must be familiar with basic Oracle database concepts and Structured Query Language.[14]

IT Audit Tools for New Auditors

COBIT 4.0 is considered to be a vital tool for IT auditors, particularly in the “strong linkages to business objectives and goals to provide the drivers and rationale for the IT supporting process.” The text, illustrations, and diagrams have been updated from earlier editions, and these changes have greatly enhanced the usability of the document, and the appendices provide additional IT governance processes and references.[15] In an article by Tommie Singleton, “COBIT is the most effective auditing tool available today, which can be applied to a variety of IT audit-related functions.” In support of this perspective, numerous process models (such as Committee of Sponsoring Organization of the Treadway Commission, Information Technology Infrastructure Library, British Standard 1500, and Capability Maturity Model) have been mapped to COBIT, at least in part because of the guidance it provides in assessing IT controls.[16]

ITGI: A LEADER AND A RESOURCE

The perspectives and actions of IT professionals, information security professionals, and auditors will impact the IT stance of an organization and the ability of IT to securely and consistently meet and exceed the objectives of an enterprise in a global community. ITGI has become a strategic force and a leading reference on IT-enabled business systems governance for the global business community. A corresponding effort relates to the ISACA perspective regarding the responsibilities of auditors or information security practitioners—those individuals are going to be required to support and become experts in IT governance. As a result, ITGI stands ready and continues in its research endeavors to support corporate enterprise in the utilization and protection of information resources to obtain business objectives. ISACA is prepared to provide resources to empower those individuals who must implement the enterprise objectives in their current (and in time to come) job responsibilities.[17]

REFERENCES

1. IT Governance Institute, In IT Governance Institute Brochure; Rolling Meadows, IL, 2–4.
2. IT Governance Institute, In Information Security Governance: Guidance for Boards of Directors and Executive Management; IT Governance Institute; Rolling Meadows, IL, 2001; 2.
4. IT Governance Institute, In COBIT® 4.0 Brochure; IT Governance Institute; Rolling Meadows, IL, 2.
17. Everett, C.J. President’s message. A Newsletter for Members about Entry and International Events and Programs; ISACA GLOBAL COMMUNIQUÉ, 2006, 1, 2.