



LEADING THE IT GOVERNANCE COMMUNITY

ITGI™ Enables ISO/IEC 38500:2008 Adoption



IT Governance Institute®

The IT Governance Institute (ITGI™) (www.itgi.org) is a non-profit, independent research entity that provides guidance for the global business community on issues related to the governance of IT assets. ITGI was established by the non-profit membership association ISACA in 1998 to help executives and IT professionals ensure that IT delivers value and its risks are mitigated through alignment with enterprise objectives, IT resources are properly managed, and IT performance is measured. ITGI developed *Control Objectives for Information and related Technology* (COBIT®) and Val IT™, and offers original research and case studies to help enterprise leaders and boards of directors fulfil their IT governance responsibilities and help IT professionals deliver value-adding services.

Disclaimer

ITGI has designed and created this publication, titled *ITGI™ Enables ISO/IEC 38500:2008 Adoption* (the 'Work'), primarily as an educational resource. ITGI makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information procedure or test, control professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology (IT) environment.

Reservation of Rights

© 2009 ITGI. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without the prior written authorisation of ITGI. Reproduction and use of all portions of this publication are permitted solely for academic, internal and non-commercial use, and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

IT Governance Institute

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: info@itgi.org
Web site: www.itgi.org

Acknowledgements

ITGI wishes to recognise:

Researcher

Gary Hardy, CGEIT, IT Winners, South Africa

Expert Reviewers

Gregory T. Grocholski, CISA, The Dow Chemical Company, USA

Tony Hayes, FCPA, Queensland Government, Australia

John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA

Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia

Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia

Robert E. Stroud, CA Inc., USA

John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

Vatsaraman Venkatakrishnan, CISA, CISM, CGEIT, ACA, Emirates Airlines, UAE

ITGI Board of Trustees

Lynn Lawton, CISA, FBCS, FCA, FIIA, KPMG LLP, UK, International President

George Ataya, CISA, CISM, CGEIT, CISSP, ICT Control SA, Belgium, Vice President

Yonosuke Harada, CISA, CISM, CAIS, InfoCom Research Inc., Japan, Vice President

Howard Nicholson, CISA, CGEIT, City of Salisbury, Australia, Vice President

Jose Angel Pena Ibarra, CGEIT, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President

Robert E. Stroud, CA Inc., USA, Vice President

Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP (retired), USA, Vice President

Frank Yam, CISA, CIA, CCP, CFE, CFS, FFA, FHKCS, FHKIoD, Focus Strategic Group, Hong Kong, Vice President

Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President

Everett C. Johnson Jr., CPA, Deloitte & Touche LLP (retired), USA, Past International President

IT Governance Committee

Tony Hayes, FCPA, Queensland Government, Australia, Chair

Sushil Chatterji, Edutech Enterprises, Singapore

Kyung-Tae Hwang, CISA, Dongguk University, Korea

John W. Lainhart IV, CISA, CISM, CGEIT, IBM Business Consulting Services, USA

Hugh Penri-Williams, CISA, CISM, CCSA, CIA, Accenture Technology Services, France

Gustavo Adolfo Solis Montes, CISA, CISM, Grupo Cynthus, Mexico

Robert E. Stroud, CA Inc., USA

John Thorp, CMC, I.S.P., The Thorp Network Inc., Canada

Wim Van Grembergen, Ph.D., University of Antwerp Management School and IT Alignment and Governance Research Institute, Belgium

ITGI Affiliates and Sponsors

American Institute of Certified Public Accountants

ASIS International

The Center for Internet Security

Commonwealth Association for Corporate Governance Inc.

FIDA Inform

Information Security Forum

Information Systems Security Association

Institut de la Gouvernance des Systemes d'Information

Institute of Management Accountants Inc.

ITGI Affiliates and Sponsors (cont.)

ISACA

ISACA chapters

ITGI Japan

Norwich University

Socitm Performance Management Group

Solvay Brussels School of Economics and Management

University of Antwerp Management School

Aldion Consulting Pte. Ltd.

Analytix Holdings Pty. Ltd.

BWise B.V.

CA Inc.

Consult2Comply

Hewlett-Packard

IBM

ITpreneurs Nederlands B.V.

LogLogic Inc.

Phoenix Business and Systems Process Inc.

Project Rx Inc.

Symantec Corp.

TruArx Inc.

Wolcott Group LLC

World Pass IT Solutions

Introduction

The need to drive more value from IT investments and manage an increasing array of IT-related risks has never been higher.

Effective enterprise governance of IT will result in improved performance and compliance with external requirements.

In 1998 ISACA¹ identified a need to improve the way enterprises governed the use of information and related technology (IT) and, in a ground-breaking move, created the IT Governance Institute (ITGI) to progress research and develop guidance in this key area of enterprise governance. ITGI (www.itgi.org) was established to advance international thinking and guidance in evaluating, directing and monitoring an enterprise's use of IT.

ITGI welcomed ISO's release of a new standard, *ISO/IEC 38500:2008 Corporate governance of information technology*, marking a global recognition of the importance of this topic and the need to formalise its adoption. At a time when the significance of information and technology is all around us, in every aspect of business and public life, the need to drive more value from IT investments and manage an increasing array of IT-related risks has never been greater. Increasing regulation is also driving heightened awareness amongst directors of the importance of a well-controlled IT environment and the need to comply with legal, regulatory and contractual obligations. Effective enterprise governance of IT will result in improved performance and compliance to external requirements.

ITGI believes that an international standard provides a foundation for further development of governance, particularly since it is applicable to all organisations, from the smallest to the largest, regardless of purpose or design. However, for effective adoption, the standard requires more implementation support. ITGI's family of products can provide such support in a way that can be tailored for enterprises of all sizes.

¹ ISACA[®] was founded in 1969 and currently has more than 86,000 constituents in more than 160 countries. ISACA is a recognised worldwide leader in IT governance, control, security and assurance. ISACA sponsors international conferences, publishes the *ISACA Journal*[®], and develops international information systems auditing and control standards. It also administers three globally respected designations: Certified Information Systems Auditor[™] (CISA[®]), Certified Information Security Manager[®] (CISM[®]) and Certified in the Governance of Enterprise IT[™] (CGEIT[™]).

ITGI's Unique Professional Approach

ISACA recognised in the early 1990s that auditors, who had their own checklists for assessing IT controls and effectiveness, were talking a different language from that used by business managers and IT practitioners. To bridge this communication gap, COBIT was created as an IT control framework for business managers, IT managers and auditors based on a generic set of IT processes meaningful to both IT professionals and business management.

ITGI's guidance, centred on the COBIT and Val IT frameworks, enables enterprise directors and managers to better understand how to direct and manage the enterprise's use of IT.

Leveraging ISACA's unique membership base of IT governance, control, security and assurance professionals and the practical experiences of hundreds of global experts, ITGI has created industry-leading guidance based on the COBIT framework, including the recently released Val IT™ framework, providing a common language and approach helping thousands of enterprises around the world understand and apply IT governance principles in practice. As a non-profit organisation, ITGI has created broad practices that are independent of any specific technology, vendor or commercial product, and has made this guidance freely available. This helps enterprise boards, executives, directors and management implement structures, processes and tools to enable them to understand and direct important IT-related requirements, monitor and evaluate critical IT activities, and make informed decisions.

Enterprises need confidence that they can rely on information systems and the information produced by those systems. They need to be able to count on a positive return from IT investments. ITGI's guidance, centred on the COBIT and Val IT frameworks, enables enterprise directors and managers to better understand how to direct and manage the enterprise's use of IT and the standard of good practice to be expected from IT providers. COBIT and Val IT provide the tools to direct and oversee all IT-related activities.

A description of all the IT governance products provided by ITGI is included at the end of this publication.

Benefit of the ISO/IEC 38500 Standard

ISO/IEC 38500 is beneficial for a number of reasons:

- It highlights the importance of IT governance due to the risks involved and significant investments required.
- It encourages enterprises to use appropriate standards to underpin their governance of IT.
- It provides a framework of six basic principles for directors to use when evaluating, directing and monitoring the use of IT in their enterprises. Following these principles will assist directors in balancing risks and encouraging opportunities arising from the use of IT.
- It is applicable for all enterprises, from the smallest to the largest, regardless of purpose, design and ownership structure.
- It makes clear that proper enterprise governance of IT may assist directors in assuring conformance with obligations (regulatory, legislation, common law, contractual) concerning the acceptable use of IT and ensuring that IT use contributes positively to the performance of the enterprise.
- It also makes clear that inadequate IT systems can expose the directors to the risk of not complying with an increasingly wide range of legislation.

Implementing the standard and responding to the direction established by the board of directors are supported by additional guidance from ITGI.

How ITGI Supports the Standard

The following summarises how COBIT, Val IT and related guidance support adoption of the standard's principles and implementation approach. For more information, a list of currently available products and web links is included at the end of this document. The new standard, *ISO/IEC 38500:2008—Corporate governance of information technology*, is based upon six key principles. The practical implications of each principle are explained below, together with how ITGI's guidance enables good practice.

The Standard's Principles²

Principle 1—Responsibility

Appropriate governance organisational structures, roles and responsibilities are required to be mandated from the executive, providing clear ownership and accountability for important decisions and tasks.

What this means in practice: The business (customer) and IT (provider) should collaborate in a partnership model utilising effective communications based on a positive and trusted relationship and demonstrating clarity regarding responsibility and accountability. For larger enterprises, an IT executive committee (often referred to as the IT strategy committee) acting on behalf of the board and chaired by a board member is a very effective mechanism for evaluating, directing and monitoring the use of IT in the enterprise and for advising the board on critical IT issues. Directors of small and medium-sized enterprises with a simpler command structure and shorter communication paths need to take a more direct approach when overseeing IT activities. In all cases, appropriate governance organisational structures, roles and responsibilities are required to be mandated from the executive, providing clear ownership and accountability for important decisions and tasks. This should include relationships with key third-party IT service providers.

How ITGI's guidance enables good practice:

- The *Board Briefing on IT Governance* and *Unlocking Value: An Executive Primer on the Critical Role of IT Governance, 2nd Edition* publications provide guidance on the roles and responsibilities for IT governance in the business and for the IT function, whether in-house or outsourced, and describe how to establish an effective IT executive (strategy) committee.
- The COBIT and Val IT frameworks include RACI³ charts showing example roles and responsibilities for board members and management for all key IT-related processes and activities.
- The *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition* explains the responsibilities of stakeholders and other involved parties when implementing or enhancing IT governance arrangements.

² For the definitions of the six principles discussed in this section, please refer to the ISO/IEC 38500–2008 standard, which may be purchased from an authorized body, such as ANSI, 25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, <http://webstore.ansi.org> or other authorized seller.

³ RACI charts outline who is Responsible, Accountable, Consulted and Informed for a task.

- COBIT’s Monitor and Evaluate (ME) processes explain the director’s role in monitoring and evaluating IT governance and IT performance with a generic method for establishing goals and objectives and related metrics. ME4 *Monitor and evaluate IT governance* specifically focuses on the oversight of IT governance activities.

Principle 2—Strategy

What this means in practice: IT strategic planning is a complex and critical undertaking requiring close co-ordination amongst enterprise-wide, business unit and IT strategic plans. It is also vital to prioritise the plans most likely to achieve desired benefits and to allocate resources effectively. High-level goals need to be translated into achievable tactical plans, ensuring minimal failures and surprises. The goal is to deliver value in support of strategic objectives while considering the associated risks in relation to the board’s appetite for taking risks. While it is important to cascade plans in a top-down fashion, the plans must also be flexible and adaptable to meet rapidly changing business requirements and IT opportunities.

The goal is to deliver value in support of strategic objectives while considering the associated risks in relation to the board’s appetite for taking risks.

Furthermore, the presence or absence of IT capabilities can either enable or hinder business strategies; therefore, IT strategic planning should include transparent and appropriate planning of IT capabilities. This should include assessment of the ability of the current IT infrastructure and human resources to support future business requirements and consideration of future technological developments that might enable competitive advantage and/or optimise costs. IT resources include relationships with many external product vendors and service providers, some of whom likely play a critical role in supporting the business. Governance of strategic sourcing is thus a very significant strategic planning activity requiring executive-level direction and oversight.

How ITGI’s guidance enables good practice:

- *The Board Briefing on IT Governance, 2nd Edition* and *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* publications explain how the IT executive (strategy) committee should enable effective strategic planning in alignment with enterprise-wide strategic planning and how business and IT management should work together to achieve successful outcomes.
- Val IT provides specific guidance on managing IT investments and (specifically, in the Investment Management [IM] domain) how strategic objectives should be supported by appropriate business cases.
- COBIT’s Plan and Organise (PO) domain explains the processes required for the effective planning and organisation of internal and external IT resources, including strategic planning, technology and architecture planning, organisational planning, investment planning, risk management, quality management and project management. The alignment of business and IT goals is also explained, with generic examples showing how they support strategic objectives for all IT-related processes based on industry-wide research.

- *Identifying and Aligning Business Goals and IT Goals* presents a better understanding of the cascading relationship among business goals, IT goals and IT processes. It presents a solid and strong list of 17 generic business goals and 18 generic IT goals, validated and prioritized among different sectors. Together with the linking information between both, it provides a good basis upon which to build a generic cascade from business goals to IT goals. A strong list of the most important business and IT goals was identified among the different sectors and further analysis by sector and geographic location identified interesting deviations, which increases the practical relevance for enterprises operating in a specific sector that want to use these lists to help them identify a good set of business/IT goals.
- *Understanding How Business Goals Drive IT Goals* is a white paper that summarizes the material in the complete research report *Identifying and Aligning Business Goals and IT Goals*.

Principle 3—Acquisition

Implementation is also not just a technology issue but rather a combination of organisational change, revised business processes, training and enabling the change.

What this means in practice: IT solutions exist to support business processes and therefore care must be taken not to consider IT solutions in isolation or as just a ‘technology’ project or service. On the other hand, an inappropriate choice of technology architecture, a failure to maintain a current and appropriate technical infrastructure, or an absence of skilled human resources can result in project failure, an inability to sustain business operations or a reduction in value to the business. Acquisitions of IT resources should be considered as a part of wider IT-enabled business change. The acquired technology must also support and operate with existing and planned business processes and IT infrastructures. Implementation is also not just a technology issue but rather a combination of organisational change, revised business processes, training and enabling the change. Therefore, IT projects should be undertaken as part of wider enterprise-wide change programmes that include other projects satisfying the full range of activities required to help ensure a successful outcome.

How ITGI’s guidance enables good practice:

- In the IM domain, Val IT provides guidance on governing and managing IT-enabled business investments through their complete life cycle (acquisition, implementation, operation and decommissioning). The Portfolio Management (PM) domain addresses how to apply effective portfolio and programme management of such investments to help ensure that benefits are realised and costs are optimised.
- COBIT’s PO domain provides guidance for planning for acquisition, including investment planning, risk management, programme and project planning, and quality planning.
- COBIT’s Acquire and Implement (AI) domain provides guidance on the processes required to acquire and implement IT solutions, covering defining requirements, identifying feasible solutions, preparing documentation, and training and enabling users and operations to run the new systems. In

addition, guidance is provided to help ensure that the solutions are tested and controlled properly as the change is applied to the operational business and IT environment.

- The ME domain includes guidance on how directors can monitor and evaluate the acquisition process, and internal controls to help ensure that acquisitions are properly managed and executed.

Principle 4—Performance

What this means in practice: Effective performance measurement depends on two key aspects being addressed: the clear definition of performance goals and the establishment of effective metrics to monitor achievement of goals. A performance measurement process is also required to help ensure that performance is monitored consistently and reliably. Effective governance is achieved when goals are set from the top down and aligned with high-level approved business goals, and metrics are established from the bottom up and aligned in a way that enables the achievement of goals at all levels to be monitored by each layer of management. Two critical governance success factors are the approval of goals by stakeholders, and the acceptance of accountability for achievement of goals by directors and managers. IT is a complex and technical topic; therefore, it is important to achieve transparency by expressing goals, metrics and performance reports in language meaningful to the stakeholders so that appropriate actions can be taken.

Two critical governance success factors are the approval of goals by stakeholders, and the acceptance of accountability for achievement of goals by directors and managers.

How ITGI's guidance enables good practice:

- The COBIT and Val IT frameworks provide generic examples of goals and metrics for the full range of IT-related processes and show how they relate to business goals, enabling enterprises to adapt them for their own specific use.
- COBIT provides management with guidance on setting IT objectives in alignment with business goals and describes how to monitor performance of these objectives using goals and metrics. Capability can be benchmarked using maturity models and control objectives.

Two key COBIT processes provide specific guidance:

- PO1 *Define a strategic IT plan* focuses on setting goals.
- Deliver and Support (DS) 1 *Define and manage service levels* focuses on defining appropriate services and service goals and documenting them in service level agreements.

In process ME1 *Monitoring and evaluating IT performance*, COBIT provides guidance on responsibilities of executive management for this activity.

COBIT provides guidance on monitoring IT governance itself in process ME4 *Monitoring and evaluating IT governance*.

- Val IT provides specific guidance and examples for monitoring the performance of an IT investment through its entire economic life cycle from

business case to benefit realisation.

- The *IT Assurance Guide: Using COBIT* explains how assurance professionals can provide independent assurance to directors regarding IT performance.

Principle 5—Conformance

What this means in practice: In today's global marketplace, enabled by the Internet and advanced technologies, enterprises need to comply with a growing number of legal and regulatory requirements. Because of corporate scandals and financial failures in recent years, there is a heightened awareness in the boardroom of the existence and implications of tougher laws and regulations. Stakeholders require increased assurance that enterprises are complying with laws and regulations and conforming to good corporate governance practice in their operating environment. In addition, because IT has enabled seamless business processes between enterprises, there is also a growing need to help ensure that contracts include important IT-related requirements in areas such as privacy, confidentiality, intellectual property and security.

IT-enabled change, including IT governance itself, usually requires significant cultural and behavioural change within enterprises as well as with customers and business partners.

Directors need to ensure that compliance with external requirements is dealt with as a part of strategic planning rather than as a costly afterthought. They also need to set the tone at the top and establish policies and procedures for their management and staff to follow, to ensure that the goals of the enterprise are realised, risks are minimised and compliance is achieved. Top management must strike an appropriate balance between performance and conformance, ensuring that performance goals do not jeopardise compliance and, conversely, that the conformance regime is appropriate and does not overly restrict the operation of the business.

How ITGI's guidance enables good practice:

- COBIT's control objectives and control practices provide a basis for establishing an appropriate control environment and assessing the adequacy of IT controls in the enterprise. The maturity models enable management to evaluate and benchmark IT process capability.
- COBIT process PO1 *Define a strategic IT plan* helps ensure that there is alignment between the IT plan and the overall business objectives, including governance requirements.
- COBIT process ME2 *Monitor and evaluate IT controls* enables directors to assess whether controls are adequate to meet compliance requirements.
- COBIT process ME3 *Ensure compliance with external requirements* helps ensure that external compliance requirements are identified, directors set the direction for compliance, and IT compliance itself is monitored, assessed and reported as a part of overall conformance to enterprise requirements.
- The *IT Assurance Guide: Using COBIT* explains how auditors can provide independent assurance of compliance and adherence to internal policies derived from internal directives or external legal, regulatory or contractual requirements, confirming that any corrective actions to address any

compliance gaps have been taken by the responsible process owner in a timely manner.

- Conformance also involves investment decisions. Val IT, specifically through Value Governance (VG) 1 and 3, PM1 and 4, and Investment Management (IM) 4, ensures that investments related to conformance balance the value of conformance with the risk and cost of non-conformance.

Principle 6—Human Behaviour

What this means in practice: The implementation of any IT-enabled change, including IT governance itself, usually requires significant cultural and behavioural change within enterprises as well as with customers and business partners. This can create fear and misunderstanding amongst staff, so implementation needs to be managed carefully if personnel are to remain positively engaged. Directors must clearly communicate goals and be seen as positively supporting the proposed changes. Training and skills enhancement of personnel are key aspects of change—especially given the rapidly moving nature of technology. People are affected by IT at all levels in an enterprise, as stakeholders, managers and users, or as specialists providing IT-related services and solutions to the business. Beyond the enterprise, IT affects customers and business partners and increasingly enables self service and automated inter-company transactions within countries and across borders. While IT-enabled business processes bring new benefits and opportunities, they also carry an increasing number of risks. Issues such as privacy and fraud are growing concerns for individuals, and these and other risks need to be managed if people are to trust the IT systems they use. Information systems can also dramatically affect working practices, by automating manual procedures.

Issues such as privacy and fraud are growing concerns for individuals, and these and other risks need to be managed if people are to trust the IT systems they use.

How ITGI's guidance enables good practice:

Seven Val IT and COBIT processes provide guidance on requirements relating to human behaviour:

- Val IT chapter 6, Functional Accountabilities and Responsibilities, emphasises the need to understand the changes required related to governance of investments and for the IT-enabled changes themselves.
- COBIT process PO4 *Define the IT organisation and relationships* explains how the IT organisation and related processes are developed and maintained appropriately to suit the needs and requirements of staff at all levels.
- COBIT process PO6 *Communicate management aims and direction* focuses on ensuring that goals and objectives are clearly communicated and the working culture promotes the right attitude to risk and control.
- COBIT process PO7 *Manage IT human resources* explains how the performance of individuals should be aligned with corporate goals, how IT specialist skills should be maintained, and how roles and responsibilities should be defined.
- COBIT process AI2 *Acquire and maintain application software* helps ensure design of applications that meets human operation and use requirements.
- COBIT process AI4 *Enable operation and use* helps ensure that users are

enabled to use systems effectively.

- COBIT process DS7 *Educate and train users* explains how user training needs can be identified and responded to, ensuring effective use of IT systems.
- COBIT process ME2 *Monitor and evaluate internal controls* enables directors to monitor internal controls and, specifically, to monitor human performance via supervisory reviews.

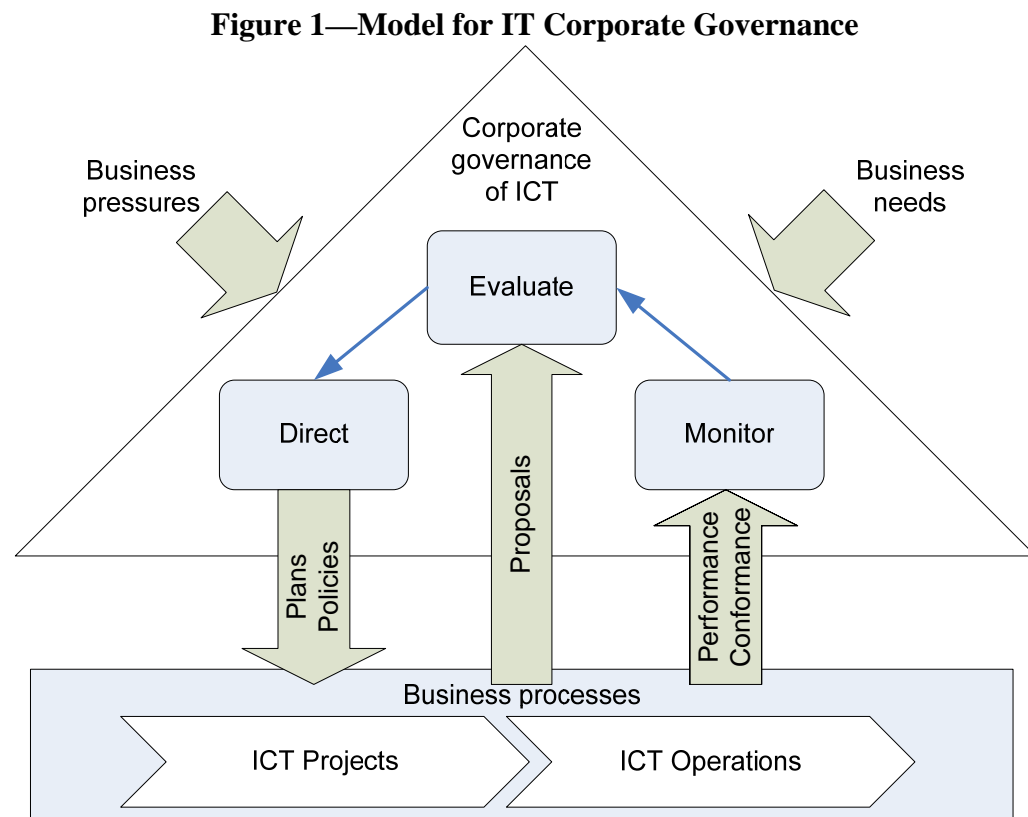
In addition, ISACA provides three certifications for professionals performing key roles related to IT governance:

- Certified in the Governance of Enterprise IT™ (CGEIT™)
- Certified Information Systems Auditor™ (CISA®)
- Certified Information Security Manager® (CISM®)

Holders of these certifications have demonstrated both capability and experience in performing such roles.

Adoption of the Standard

The good practices in COBIT are a common approach to good IT control—implemented by business and IT managers, and assessed on the same basis by auditors.



Source: © ISO. This material is reproduced from ISO/IEC 38500:2008 with permission of the American National Standards Institute (ANSI) on behalf of the International Organisation for Standardisation (ISO). No part of this material may be copied or reproduced in any form, electronic retrieval system or otherwise or made available on the Internet, a public network, by satellite or otherwise without the prior written consent of the ANSI or other authorized body. Copies of this standard may be purchased from the ANSI, 25 West 43rd Street, New York, NY 10036, USA, +1.212.642.4900, <http://webstore.ansi.org> or other authorized seller.

ISO/IEC 38500 recommends that directors should govern IT through three main tasks, as shown in **figure 1**:

- Evaluating
- Directing
- Monitoring

What this means in practice:

Implementation of an effective IT governance approach is made easier and is most effective when it:

- Is aligned with accepted corporate governance standards and practices
- Is aligned with the enterprise's approach to governance
- Covers all aspects of an enterprise's IT-related activities
- Is based on principles and objectives that can be understood and applied by all the stakeholders

Reference to available comprehensive frameworks, standards and practices and their adoption and use (tailored to reflect culture, requirements and capabilities) can efficiently and effectively support enterprises in establishing an appropriate IT governance approach.

How ITGI Guidance Enables Good Practice

The following ITGI materials support the three main tasks recommended in ISO/IEC 38500.

Evaluate:

- *The Board Briefing on IT Governance, 2nd Edition* and *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* publications describe what boards should do about IT governance, what it covers, what questions to ask, and how to compare one's own enterprise with best practice.
- COBIT and Val IT provide a basis for assessing the adequacy of IT controls and management practices and enable management to evaluate and benchmark IT process capability.
- The Identify Needs and Envision Solution phases of the *IT Governance Implementation Guide: Using COBIT[®] and Val IT, 2nd Edition* explain how to focus the evaluation of IT on business needs and critical IT processes and then how to perform a gap analysis against good practice.
- *COBIT[®] Quickstart[™], 2nd Edition* provides guidance for the smaller enterprise or for larger enterprises wishing to evaluate their control and governance of IT based on a pre-defined baseline.
- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management* helps identify triggers and evaluate business needs to better manage IT-related investments.
- *Enterprise Value: Governance of IT Investments, The Business Case* helps create a business case for improvement of IT governance.
- *The IT Assurance Guide: Using COBIT[®]* enables assurance professionals to

provide management with independent evaluations and provides a method and example tests to conduct audits and reviews.

Direct:

- The *Board Briefing on IT Governance, 2nd Edition* and *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* publications describe what boards can do about IT governance and explain how it is accomplished.
- COBIT and Val IT provide implementation guidance in the form of control objectives and key management practices that should be considered (based on generally accepted international standards and best practices) to enable good IT governance.
- The Plan Solution and Implement Solution phases of the *IT Governance Implementation Guide: Using COBIT[®] and Val IT, 2nd Edition* explain how to prioritise, plan and design IT governance improvements.
- *COBIT[®] Quickstart[™], 2nd Edition* provides a recommended baseline of controls for the smaller enterprise or for larger enterprises wishing to make an initial step towards good IT governance.
- For enterprises where security is a key area requiring improvement, *COBIT[®] Security Baseline[™], 2nd Edition* provides easy-to-follow guidance for directing the implementation of key IT security controls in alignment with the IT security standard ISO/IEC 27002.

Monitor:

- The *Board Briefing on IT Governance, 2nd Edition* and *Unlocking Value: An Executive Primer on the Critical Role of IT Governance* publications describe what boards should do to effectively monitor enterprise governance of IT.
- COBIT provides guidance in the form of recommended IT processes for monitoring and evaluating IT (ME domain) covering performance measurement, internal control effectiveness, compliance with external requirements and achievement of overall effective governance.
- COBIT and Val IT include example goals and metrics to support establishment of an effective monitoring process aligned with business goals and objectives.
- The Operationalise Solution phase of the *IT Governance Implementation Guide: Using COBIT[®] and Val IT, 2nd Edition* explains how to put IT governance into normal business operations and how to monitor and measure the success of the IT governance improvements.
- *The IT Assurance Guide: Using COBIT[®]* enables assurance professionals to provide management with independent opinions on performance and conformance and provides a method and example tests to conduct audits and reviews.

How ITGI’s Products Support Adoption of ISO/IEC 38500

Figure 2 shows how ITGI’s products support adoption of ISO/IEC 38500.

Figure 2—Relation of ITGI’s Products and ISO/IEC 38500									
ITGI Product	ISO/IEC 38500 Areas								
	Responsibility	Strategy	Acquisition	Performance	Conformance	Human Behaviour	Evaluate	Direct	Monitor
<i>Board Briefing on IT Governance, 2nd Edition</i>	√	√				√	√	√	√
<i>Unlocking Value: An Executive Primer on the Critical Role of IT Governance</i>	√	√				√	√	√	√
<i>COBIT®</i>	√	√	√	√	√	√	√	√	√
<i>Val IT™</i>	√	√	√	√	√	√	√	√	√
<i>IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition</i>							√	√	√
<i>IT Assurance Guide: Using COBIT®</i>				√	√		√		√
<i>COBIT® Quickstart™, 2nd Edition</i>							√	√	
<i>Enterprise Value: Governance of IT Investments, Getting Started With Value Management</i>							√		
<i>COBIT® Security Baseline™, 2nd Edition</i>	√						√	√	
<i>Enterprise Value: Governance of IT Investments, The Business Case</i>			√	√			√	√	√

COBIT is increasingly being adopted globally as the ‘de facto standard’ control model.

Val IT was introduced to extend ITGI guidance into the area of IT-enabled investments.

The combination of Val IT and COBIT frameworks provides a comprehensive basis for establishing effective IT governance.

The good practices in COBIT are a common approach to good IT control—implemented by business and IT managers, and assessed on the same basis by auditors. Over the years, COBIT has been developed as a freely available framework and is now increasingly being adopted globally as the ‘de facto standard’ control model for implementing and demonstrating effective IT governance and management.

Recently, Val IT was introduced to extend ITGI guidance into the area of IT-enabled investments. The combination of Val IT and COBIT provides a comprehensive basis for establishing effective governance arrangements over enterprise IT-related activities.

The COBIT framework, in versions 4.0 and higher, includes all of the following:

- Framework—Explains how COBIT organises IT governance management and control objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility and measure performance
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:

- *Unlocking Value: An Executive Primer on the Critical Role of IT Governance*—Provides executives with an insight into why IT governance is important and how it can add value to the enterprise
- *Board Briefing on IT Governance, 2nd Edition*—Helps executives better understand IT governance concepts, what the issues are and how best to make them happen
- COBIT Online[®]—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking, and a discussion facility for sharing experiences and questions.
- *COBIT[®] Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective
- *IT Assurance Guide: Using COBIT[®]*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It is also useful for performing self-assessments against the control objectives in COBIT 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Control Objectives for Basel II—The Importance of Governance and Risk Management for Compliance*—Provides guidance for banks on operational risks relating to IT
- *IT Governance Implementation Guide: Using COBIT[®] and Val IT, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit

- *COBIT® Quickstart™, 2nd Edition*—Provides a baseline of control for the smaller enterprise and a possible first step for the larger enterprise
- *COBIT® Security Baseline™, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise
- COBIT Mappings—Currently posted at www.isaca.org/downloads:
 - *Aligning COBIT® 4.1, ITIL v3 and ISO/IEC 27002 for Business Benefit*
 - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
 - *COBIT® Mapping: Mapping of CMMI® for Development V1.2 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT®, 2nd Edition*
 - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of ITIL With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of NIST SP800-53 With COBIT® 4.1*
 - *COBIT® Mapping: Mapping of PMBOK With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of PRINCE2 With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.0*
 - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT® 4.0*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems.

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:

- *Enterprise Value: Governance of IT Investments, Getting Started With Value Management*—This publication provides an easy-to-follow guide on getting a value management initiative started for business and IT executives and organisational leaders.
- *Enterprise Value: Governance of IT Investments—The Val IT Framework 2.0*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
 - Three processes—Value Governance, Portfolio Management and Investment Management
 - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as do COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters and other framework-specific information, visit www.itgi.org, www.isaca.org/cobit and www.isaca.org/valit.