

ITGI Enables ISO/IEC 38500:2008 Adoption

Excerpted and reprinted from *ITGI™ Enables ISO/IEC 38500:2008 Adoption*, ITGI, 2009. The full text of this publication is available as a complimentary download at www.isaca.org/downloads.

Gary Hardy, CGEIT, is director of IT Winners, an independent consultancy based in South Africa. He has been involved in the IT industry for more than 30 years and is a longstanding member of ISACA. He has worked in a variety of IT roles, initially as a systems developer and project manager, then as a computer audit manager for a major oil company and group manager at Deloitte & Touche in London. He has been director of consultancy for a major IT security company and a director of risk consulting at Arthur Andersen. He is currently an advisor to the ITGI and Deloitte, a thought leader on IT governance and an author of many publications on related topics.

The recent release of a new standard, ISO/IEC 38500:2008 ‘Corporate Governance of Information Technology’, by the International Organisation for Standardisation (ISO) and the International Electrotechnical Commission (IEC), marks the global recognition of the importance of this topic and the need to formalise its adoption.

SIX PRINCIPLES OF THE STANDARD

The new standard is based upon six key principles.

Principle 1—Responsibility

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. 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.

Principle 2—Strategy

IT strategic planning is a complex and critical undertaking requiring close co-ordination amongst enterprise-wide, business unit and IT strategic plans. High-level goals need to be translated into achievable tactical plans, ensuring minimal failures and surprises. 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 play a critical role in supporting the business. Thus, governance of strategic sourcing is a significant strategic planning activity requiring executive-level direction and oversight.

Principle 3—Acquisition

Acquisitions of IT resources should be considered as part of a wider IT-enabled business change. The acquired technology must also support and operate within existing and planned business processes and IT infrastructures. Implementation is not just a technology issue but a combination of organisational change, revised business processes, training and enabling the change. 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.

Principle 4—Performance

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.

Principle 5—Conformance

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. 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.

Directors 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.

Principle 6—Human Behaviour

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. Directors must clearly

communicate goals, provide personnel training and skill enhancement, and be seen as positively supporting the proposed changes.

OTHER RECOMMENDATIONS

Additionally, ISO/IEC 38500 recommends that directors govern IT through three main tasks: evaluating, directing and monitoring.

As a global thought leader in the area of IT governance since 1998, the IT Governance Institute® (ITGI™) has long produced guidance surrounding and supporting the principles espoused in the new standard. **Figure 1** shows how ITGI's products support adoption of ISO/IEC 38500.

The practices in *Control Objectives for Information and related Technology* (COBIT)—implemented by business and IT managers and assessed on the same basis by auditors—are a common approach to IT control. 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 IT¹ 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.

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.

ENDNOTES

¹ Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Figure 1—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>			√	√			√	√	√