



Come join the discussion! Delton Sylvester will respond to questions and comments in the [discussion area of the COBIT—Use It Effectively](#) topic beginning 21 April 2011.

## ISO 38500—Why Another Standard?

By Delton Sylvester

IT is not getting sufficient coverage in the boardroom or at executive meetings. Discussions on IT are viewed as complex and are at the wrong level. There is a need to talk about the use of technology, not the technology itself, e.g., improved productivity as opposed to the latest version of technology. IT governance is also given lip service at higher levels in the organization. Even though the board and executives outwardly support IT governance initiatives, when it comes to funding, the answer is usually along the line of “Yes, we know we should do this; we just do not have the budget.”

Additionally, failures in projects and operational disruptions continue even though processes (developed using COBIT) or management tools are in place. Often, these failures can be directly attributed to poorly informed decisions made at the board or executive level. Business sees information technology as an IT department responsibility instead of as a corporate asset. ISO 38500 positions IT at a strategic level and looks at it from a demand standpoint (“how can we use IT?” rather than “how do we deliver IT?”). It also places emphasis on the board’s behavior around the use of IT.

### ISO 38500 Vs. COBIT Vs. ITIL

ISO 38500<sup>1</sup> looks down from the top, much like a roof on a house. COBIT (the what) is the walls, and process frameworks such as ITIL and Projects in Controlled Environments 2 (PRINCE2) (the how) are the foundation. Using the house analogy, if the board tried to implement the roof, ISO 38500, without the foundation or walls, it would collapse. Furthermore, without the roof, enterprises would be exposed to the elements. ISO 38500 is not one size fits all. It does not replace COBIT, ITIL, or other standards or frameworks, but, rather, it complements them by providing a demand-side-of-IT-use focus.

### Overview of ISO 38500

The objective of ISO 38500 is to provide a structure of principles for directors (including owners, board members, directors, partners and senior executives) to use when evaluating, directing and monitoring the use of IT in their organizations. This standard provides a structure for effective governance of IT to assist those at the highest level of organizations to understand and fulfill their legal, regulatory and ethical obligations regarding their organizations’ use of IT. The scope of the standard is to provide guiding principles for directors of organizations on the effective, efficient and acceptable use of IT within their organizations. It is applicable for all organizations, from the smallest to the largest, regardless of purpose, design or ownership structure.

### The Model

Directors should govern IT through three main tasks:<sup>2</sup>

1. Evaluate the current and future use of IT.
2. Direct preparation and implementation of plans and policies to ensure that the use of IT meets business objectives.
3. Monitor conformance to policies and performance against the plans.

The standard sets out six principles for good corporate governance of IT. The principles express preferred behavior to guide decision making. The statement of each principle refers to what should happen, but does not prescribe how, when or by whom the principles would be implemented; these aspects are dependent on the nature of the organization implementing the principles. It is similar to a capability maturity model description of an ideal state.

Each of the principles is then tied into the model to provide a best practice for each principle (**figure 1**).

## Implementation Readiness

As ISO 38500 is driven from the top down, IT departments need to make sure that they are ready for the new demands the board will pose (e.g., performance measurements, clear governance mechanisms). Initially, an assessment of readiness from an IT point of view would be a good idea so that the department is not found wanting, should the board adopt the standard. In principle, if COBIT maturity is high for governance processes, e.g., PO1, PO4, ME1, ME4, the department should be in a good

position. These processes were chosen because they deal mostly with governance and provide a link to ISO 38500. It would be a good idea to develop a checklist using COBIT to address the six principles of ISO 38500. The IT director should understand the requirements of ISO 38500 and begin driving the readiness.

## Tips for Implementing ISO 38500

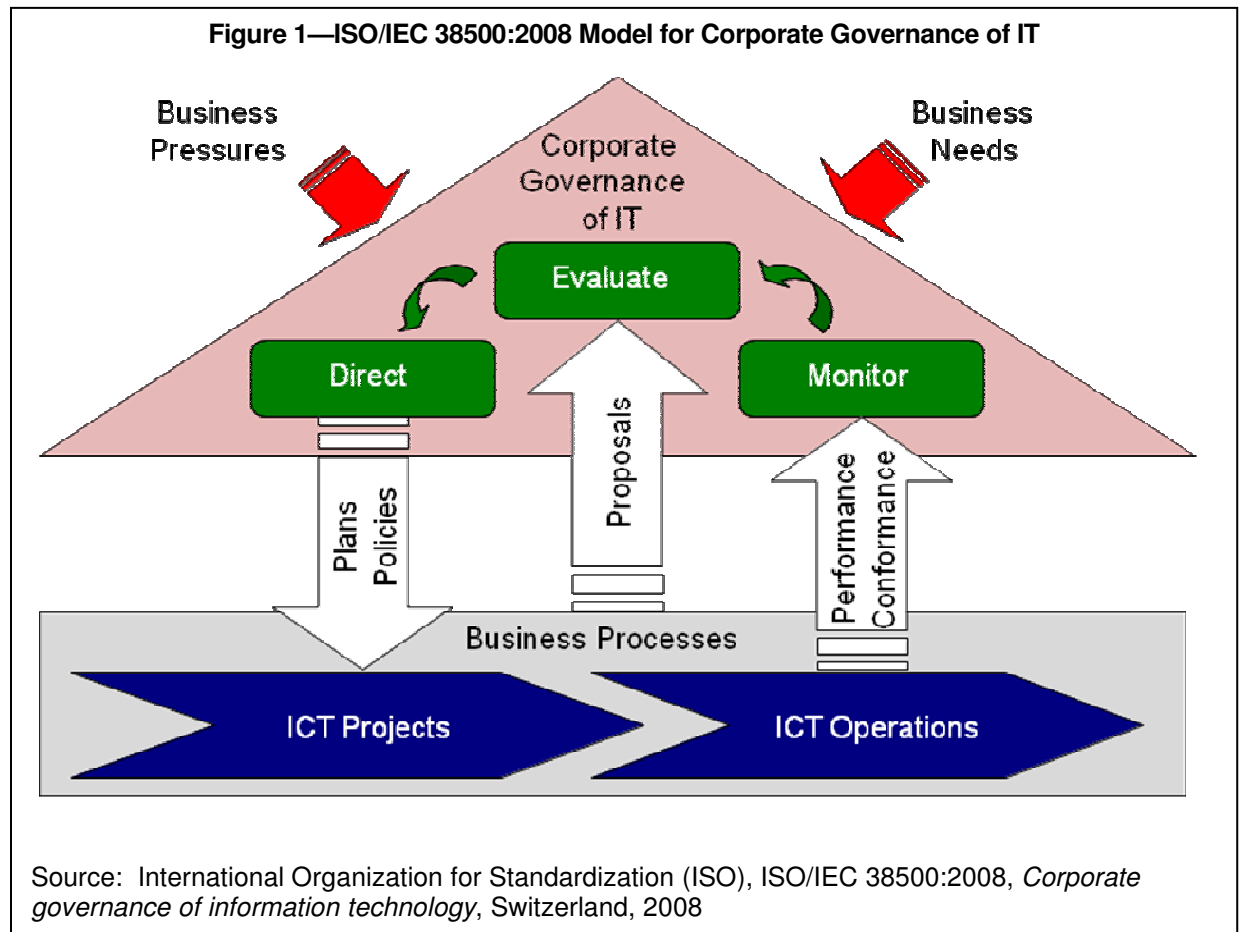
- Make ISO 38500 a board and executive management priority, if it is to succeed. IT governance must be directed from the top.
- Make IT governance part of the IT strategy, which is, in turn, part of the business strategy.
- Look for tangible benefits as opposed to “compliance for compliance’s sake.”
- Acknowledge the people factor, and incorporate it into key performance indicators (KPIs).
- Prioritize IT governance activities with clear milestones.

## Acknowledgement

The figure from ISO/IEC 38500:2008, *Corporate governance of information technology*, is reproduced with the permission of the International Organization for Standardization (ISO). This standard can be obtained from any ISO member and from the web site of the ISO Central Secretariat at the following address: [www.iso.org](http://www.iso.org). Copyright remains with ISO.

## Delton Sylvester

has more than 10 years of experience in the IT industry, with a key focus on project management and the governance of IT including COBIT, IT strategy, IT architecture and process design. Sylvester is considered a subject matter expert (SME) on COBIT and is often called on to assist with COBIT implementations. He was part of a team of 40 experts worldwide who updated COBIT to its current version. Sylvester was one of the pioneers in implementing COBIT within South Africa at De Beers from 2000 to 2003 and played a key role in the South African Revenue Services’ governance of IT program, hosting a



disaster management course that prepared delegates to handle disasters within their organization. He currently travels across Africa consulting for the Central Banks of the South African Development Community (SADC) and East Africa and a few commercial banks in the Southern African Region.

## Endnotes

<sup>1</sup> International Organization for Standardization (ISO), ISO/IEC 38500:2008, *Corporate governance of information technology*, Switzerland, 2008

<sup>2</sup> *Ibid.*

*COBIT Focus* is published by ISACA. Opinions expressed in *COBIT Focus* represent the views of the authors. They may differ from policies and official statements of ISACA and its committees, and from opinions endorsed by authors, employers or the editors of *COBIT Focus*. *COBIT Focus* does not attest to the originality of authors' content.

© 2011 ISACA. All rights reserved.

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. Please contact Julia Fullerton at [jfullerton@isaca.org](mailto:jfullerton@isaca.org).

### Framework Committee

Patrick Stachtchenko, CISA, CGEIT, CA, France, chair  
Steven A. Babb, CGEIT, UK  
Sushil Chatterji, CGEIT, Singapore  
Sergio Fleginsky, CISA, Uruguay  
John W. Lainhart IV, CISA, CISM, CGEIT, USA  
Mario C. Micallef, CGEIT, CPAA, FIA, Malta  
Derek J. Oliver, Ph.D., DBA, CISA, CISM, CITP, FBCS, FISM, UK  
Robert G. Parker, CISA, CA, CMC, FCA, Canada  
Jo Stewart-Rattray, CISA, CISM, CGEIT, CSEPS, Australia  
Robert E. Stroud, CGEIT, USA  
Rolf M. von Roessing, CISA, CISM, CGEIT, Germany

### Editorial Content

Comments regarding the editorial content may be directed to Jennifer Hajigeorgiou, senior editorial manager, at [jhajigeorgiou@isaca.org](mailto:jhajigeorgiou@isaca.org).



©2011 ISACA. All rights reserved.