DOI:10.1145/2656385

Business leaders may bemoan the burdens of governing IT, but the alternative could be much worse.

BY CARLOS JUIZ AND MARK TOOMEY

To Govern IT, or Not to Govern IT?

TO GOVERN, OR not to govern information technology (IT) is no longer a choice for any organization. IT is a major instrument of business change in both private- and public-sector organizations. Without good governance, organizations face loss of opportunity and potential failure. Effective governance of IT promotes achievement of business objectives, while poor governance of IT obstructs and limits such achievement.

The need to govern IT follows from two strategic factors: business necessity and enterprise maturity. Business necessity follows from many actors in the market using technology to gain advantage. Consequently, being relevant and competitive requires organizations to deeply integrate their own IT agendas and strategic business plans to ensure appropriate positioning of technology opportunity and response to technology-enabled changes in the marketplace. Enterprise maturity follows from a narrow focus on operating infrastructure, architecture, and service management of an owned IT asset no longer being key to development of the organization. Achieving value involves more diverse arrangements for sourcing, ownership, and control in which the use of IT assets is not linked to direct administration of IT assets. Divestment activities (such as outsourcing and adoption of cloud solutions) increasingly create unintended barriers to flexibility, as mature organizations respond to new technology-enabled pressure. Paradoxically, contemporary sourcing options (such as cloud computing and software-as-a-service) can increase flexibility and responsiveness. Business necessity and enterprise maturity thus overlap and feed each other.

The International Standard for Corporate Governance of Information Technology ISO/IEC 38500[3] was developed in 2008 by experts from government and industry (http://www.iso.org) who understand the importance of resetting the focus for governance of IT on business issues without losing sight of technology issues. While it does not say so explicitly, the standard leads to one inescapable three-part conclusion for which business leaders must assume responsibility:

Agenda. Setting the agenda for IT use as an integral aspect of business strategy;

Investment. Delivery of investments in IT-enabled business capability; and

Operations. Ongoing successful operational use of IT in routine business activity.

Implementation of effective ar-

» key insights

- **Governance of IT is a board and top-executive responsibility focusing on business performance and capability, not on technology details.**
- **A principles-based approach to the governance of IT, as described in the ISO/IEC 38500 standard, is consistent with broader models for guidance of the governance of organizations and accessible to business leaders without specific technology skills.**
- **Adopting ISO/IEC 38500 to guide governance of IT helps leaders plan, build, and run IT-enabled organizations.**

IMAGE BY ANDRIJ BORYS ASSOCIATES/SHUTTERSTOCK

rangements for governance of IT must also address the need for organizations to ensure value creation from investment in IT. Lack of good IT governance risks inappropriate investment, failure of services, and noncompliance with regulations.

Following de Haes and Van Grembergen,[2] proper governance of IT is needed to ensure investments in IT generate required business value and that risks associated with IT are mitigated. This latest consideration to value and risk is closer to the principles of good governance, but there remains in management-based published guidance on IT governance a predominantly procedural approach to the requirement for effective governance of IT.

IT Governance and Governance of IT

The notion of IT governance has existed since at least the late 1990s, producing diverse conflicting definitions. These definitions and the models that underpin them tend to focus on the supply of IT, from alignment of an organization's IT strategy to its business strategy to selection and delivery of IT projects to the operational aspects of IT systems. These definitions and models should have improved the capability of organizations to ensure their IT activities are on track to achieve their business strategies and goals. They should also have provided ways to measure IT performance, so IT governance should be able to answer questions regarding how the IT department is functioning and generating return on investment for the business.

Understanding that older definitions and models of IT governance focus on the internal activities of the IT department leads to the realization that much of what has been called "IT governance" is in fact "IT management," and confusion has emerged among senior executives and IT managers regarding what exactly is governance and management (and even operation) of IT. The reason for this confusion is that the frontiers between them may be somewhat blurred and by a propensity of the IT industry to inappropriately refer to management activities as IT governance.[12]

There is widespread recognition

that IT is not a standalone business resource. IT delivers value only when used effectively to enable business capability and open opportunities for new business models. What were previously viewed as IT activities should instead be viewed as business activities that embrace the use of IT. Governance of IT must thus include important internal IT management functions covered by earlier IT governance models, plus external functions that address broader issues of setting and realizing the agenda for the business use of IT. Governance of IT must embrace all activities, from defining intended use of IT through delivery and subsequent operation of IT-enabled business capability.

We subscribe to the definition that governance of IT is the system to direct and control use of IT. As reinforced repeatedly through major government- and private-sector IT failures, control of IT must be performed from a business perspective, not an IT perspective. This perspective, and the definition of governance of IT, requires business leaders come to terms with what they can achieve by harnessing IT to enable and enhance business capability and focus on delivering the most valuable outcomes. Governance of IT must provide clear and consistent visibility of how IT is used, supplied, and acquired for everyone in the organization, from board members to business users to IT staff members.[5]

"Governance of IT" is equivalent to "corporate governance of IT," "enterprise governance of IT," and "organizational governance of IT." Governance of IT has its origins in corporate governance. Corporate governance objectives include stewardship and management of assets and enterprise resources by the governing bodies of organizations, setting and achieving the organization's purpose and objectives, and conformance[9] by the organization with established and expected norms of behavior. Corporate governance is an important means of dealing with agency problems (such as when ownership and management interests do not match). Conflicts of interest between owners (shareholders), managers, and other stakeholders—citizens, clients, or users—can occur whenever these roles are separated.[8]

Lack of good IT governance risks inappropriate investment, failure of services, and noncompliance with regulations.

Corporate governance includes development of mechanisms to control actions taken by the organization and safeguard stakeholder interests as appropriate.[4] Private and public organizations are subject to many regulations governing data retention, confidential information, financial accountability, and recovery from disasters.[7] While no regulations require a governance-of-IT framework, many executives have found it an effective way to ensure regulatory compliance.[6] By implementing effective governance of IT, organizations establish the internal controls they need to meet the core guidelines of many regulations.

Some IT specialists mistakenly think business leaders cannot govern IT, since they lack technology skills. Understanding the capability IT brings or planning new, improved business capability enabled by smarter, more effective use of IT does not require specialized knowledge of how to design, build, or operate IT systems. A useful metaphor in this sense is the automobile; a driver need not be a designer or a manufacturing engineer to operate a taxi service but must understand the capabilities and requirements for the vehicles used to operate the service.

Governance of IT Standardization

Australian Standard AS 8015, published in 2005, was the first formal standard to describe governance of IT without resorting to descriptions of management systems and processes. In common with many broader guides for corporate governance and governance in the public sector, AS 8015 took a principles-based approach, focusing its guidance on business use of IT and business outcomes, rather than on the technical supply of IT. ISO/IEC 38500, published in 2008, was derived from AS 8015 and is the first international standard to provide guidelines for governance of IT. The wording for the definition for governance of IT in AS 8015 and its successor, ISO/IEC 38500, was deliberately aligned with the definition of "corporate governance" in the Cadbury report.[1]

Since well before release of either AS 8015 or ISO/IEC 38500, many organizations have confused governance and management of IT. This confusion is exacerbated by efforts to integrate

some aspects of governance in common de facto standards for IT management, resulting in these aspects of governance being described in management systems terms. In an effort to eliminate confusion, we no longer refer to the concept of IT governance, focusing instead on the overarching concepts for governance of IT and the detailed activities in IT management (see Figure 1).

Figure 2 outlines the final draft (issued November 2014) conceptual model for governance of IT from the proposed update of ISO/IEC 38500 and its relation with IT management. As the original ISO/IEC project editor for ISO/IEC 38500, author Mark Toomey[12] has presented evolved versions of the original ISO/IEC 38500 model that convey more clearly the distinction between governance and management activities and the business orientation essential for effective use of IT from the governance viewpoint. Figure 2 integrates Toomey's and the ISO/IEC 38500's current draft model to maximize understanding of the interdependence of governance and management in the IT context.

In the ISO/IEC 38500 model, the governing body is a generic entity (the individual or group of individuals) responsible and accountable for performance and conformance (through control) of the organization. While ISO/IEC 38500 makes clear the role of the governing body, it also allows that such delegation could result in a subsidiary entity giving more focused attention to the tasks in governance of IT (such as creation of a board committee). It also includes delegation of detail to management, as in finance and human resources. There is an implicit expectation that the governing body will require management establish systems to plan, build, and run the IT-enabled organization.

An informal interpretation of Figure 2, focused on business strategy and projects, is that there is a continuous cycle of activity that can simultaneously operate at several levels:

Evaluation. The governing body evaluates the organization's overall use of IT in the context of the business environment, directs management to perform a range of tasks relating to use of IT, and continues to monitor the use

Figure 1. Main ISO/IEC standards of IT management and governance of IT.

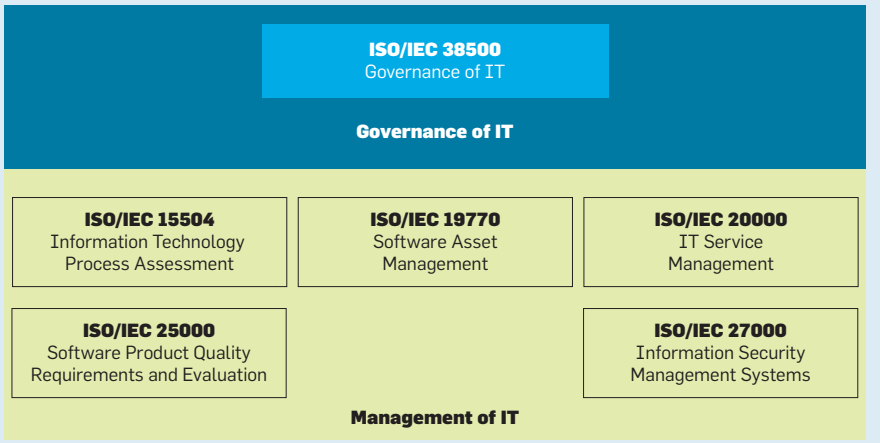
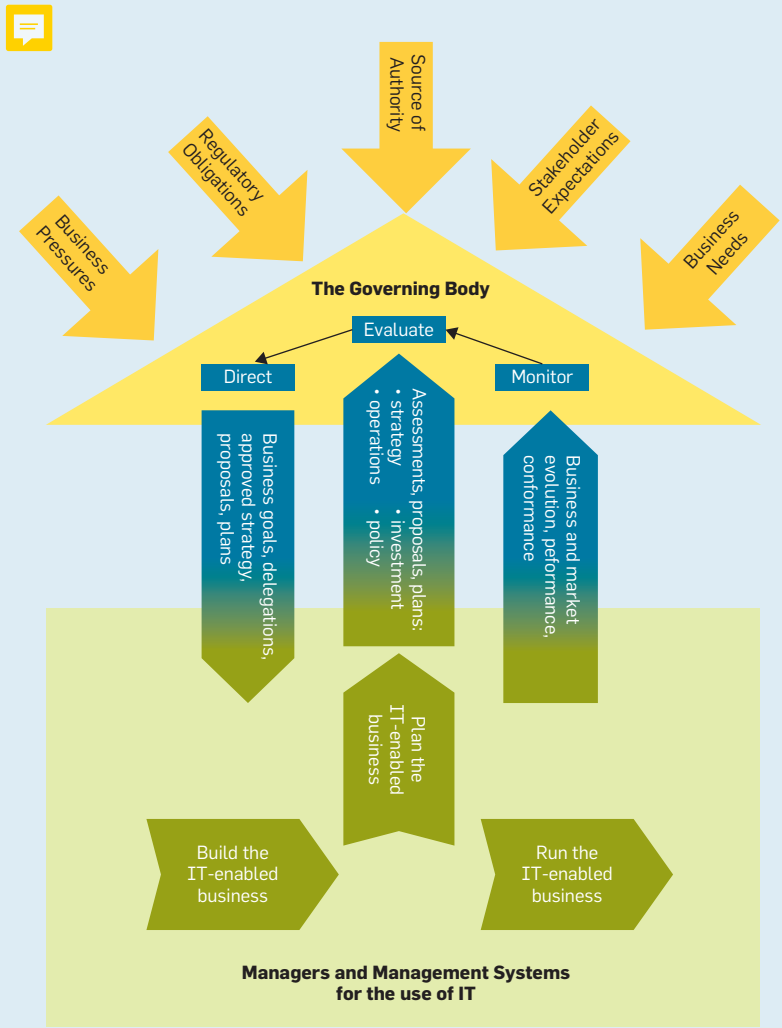


Figure 2. Model for governance of IT derived from the current Final Draft International Standard ISO/IEC 38500.[3]



of IT with regard to business and marketplace evolution;

Assessment. Business and IT units collaboratively develop assessment proposals and plans for business strategy, investment, operations, and policy for the IT-enabled business; and

Implementation. The governing body evaluates the proposed assessment proposals and plans and, where appropriate, directs that they should be adopted and implemented; the governing body then monitors implementation of the plans and policies as to whether they deliver required performance and conformance.

Regarding management scope, as outlined in Figure 2, managers must implement and run the following activities:

Plan. Business managers, supported by technology, organization development, and business-change professionals plan the IT-enabled business, as directed by the governing body, proposing strategy for the use of IT and investment in IT-enabled business capability;

Build. Investment in projects to build the IT-enabled business are undertaken as directed by and in conformance with delegation, plans, and policies approved by the board; project personnel with business-change and technology skills then work with line managers to build IT-enabled business capability;

Run. To close the virtuous cycle, once the projects become a reality, managers deliver the capability to run the IT-enabled business, supported by appropriate management systems for the operational use of IT; and

Monitor. All activities and systems involved in planning, building, and running the IT-enabled business are subject to ongoing monitoring of market conditions, performance against expectations, and conformance with internal rules and external norms.

ISO/IEC 38500 set out six principles for good corporate governance of IT that express preferred organizational behavior to guide decision making. By merging and clarifying the terms for the principles from AS 8015 and ISO/IEC 38500, we derive the following summary of the principles:

Responsibility. Establish appropriate responsibilities for decisions relating to the use and supply of IT;

Strategy. Plan, supply, and use IT to best support the organization;

Acquisition. Invest in new and ongoing use of IT;

Performance. Ensure IT performs well with respect to business needs as required;

Conformance. Ensure all aspects of decision making, use, and supply of IT conforms to formal rules; and

Human behavior. Ensure planning, supply, and use of IT demonstrate respect for human behavior.

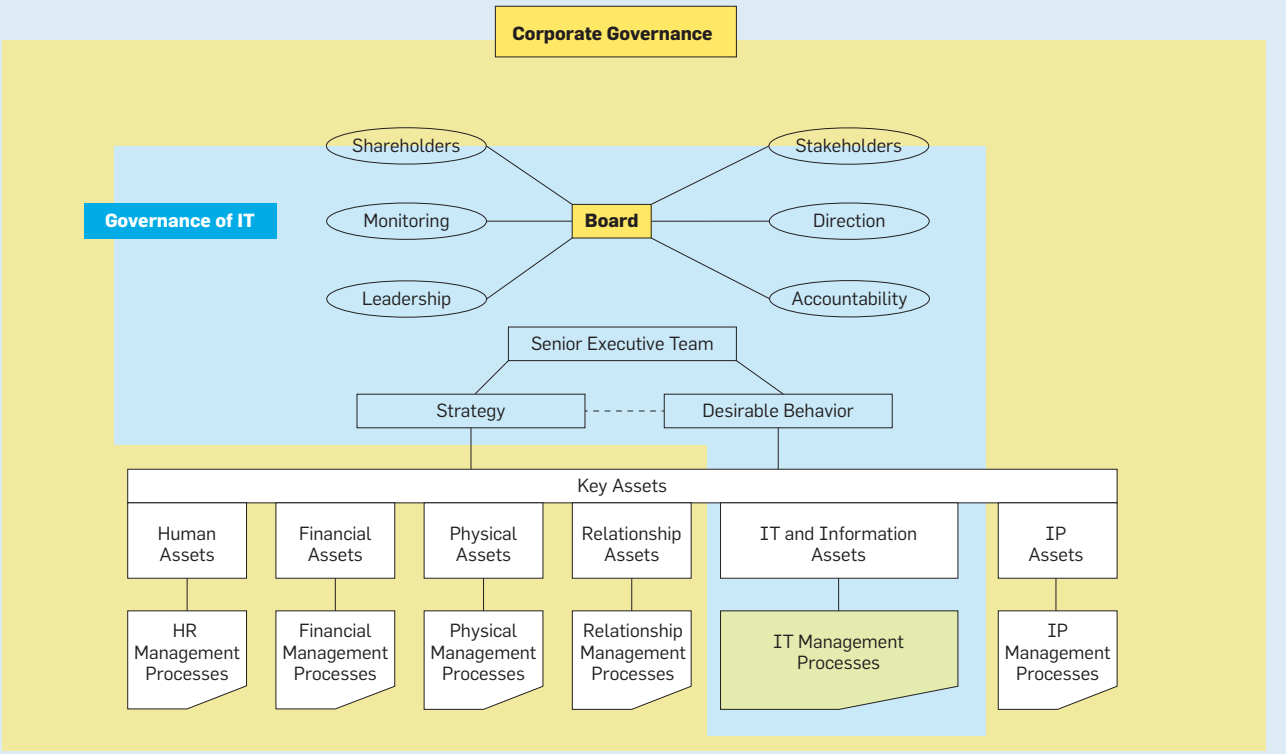
These principles and activities clarify the behavior expected from implementing governance of IT, as in Stachtchenko:[10]

Stakeholders. Stakeholders delegate accountability and stewardship to the governance body, expecting in exchange that body to be accountable for activities necessary to meet expectations;

Governance body. The governance body sets direction for management of the organization, holding management accountable for overall performance; and

Stewardship role. The governance body takes a stewardship role in the

Figure 3. Coverage area for behavior-oriented governance and management of IT, linking corporate and key assets (own elaboration from Weill and Ross[14]).



traditional sense of assuming responsibility for management of something entrusted to one's care.

Governance of IT: Process-Oriented vs. Behavior-Oriented

Van Grembergen[13] defined governance of IT as the organizational capacity exercised by the board, executive management, and IT management to control formulation and implementation of IT strategy, ensuring fusion of business and IT. Governance consists of leadership, organizational structures, and processes that ensure the organization's IT sustains and extends the organization's strategy and objectives. This definition is loosely consistent with the IT Governance Institute's definition[4] that governance of IT is part of enterprise governance consisting of leadership, organizational structures, communication mechanisms, and processes that ensure the organization's IT sustains and extends the organization's strategy and objectives. However, both definitions are more oriented to processes, structures, and strategy than the behavioral side of good governance, and, while embracing the notion that effective governance depends on effective management systems, tend to focus on system aspects rather than on true governance of IT aspects.

Weill and Ross[14] said governance of IT involves specifying the decision rights and accountability framework to produce desired behavior in the use of IT in the organization. Van Grembergen[13] said governance of IT is the responsibility of executives and senior management, including leadership, organizational structures, and processes that ensure IT assets support and extend the organization's objectives and strategies. Focusing on how decisions are made underscores the first ISO/IEC 38500 principle, emphasizing behavior in assigning and discharging responsibility is critical for deriving value from investment in IT and to the organization's overall performance.

Governance of IT must thus include a framework for organizationwide decision rights and accountability to encourage desirable behavior in the use of IT. Within the broader system for governance of IT, IT management focuses on a small but critical set of IT-related decisions, including IT principles, enterprise architecture, IT infrastructure capabilities, business application needs, and IT investment and prioritization.[14] Even though governing IT and its core is deeply behavioral, this set of IT-related decisions defines the implementation framework. These decision rights define mainly who makes decisions delegated by the governing body and what decisions they make, along with how they do it. Focusing on decision rights intrinsically defines behavioral rather than process aspects of the governance of IT.

The best process model is often readily defeated by poor human behavior.

Likewise, process-oriented IT management as described in Control Objectives for Information and Related Technology, or COBIT (http://www.isaca.org/cobit), and similar frameworks is also part of the governance of IT, ensuring IT activities support and enable enterprise strategy and achievement of enterprise objectives. However, focusing primarily on IT management processes does not ensure good governance of IT. IT management processes define mainly what assets are controlled and how they are controlled. They do not generally extend to broader issues of setting business strategy influenced by or setting the agenda for the use of IT. Nor do they extend fully into business capability development and operational management intrinsic to the use of IT in most organizations. The latest version of COBIT—COBIT 5—includes the ISO/IEC 38500 model for the first time. However, there is a quite fundamental and significant difference between ISO/IEC 38500 and COBIT 5 and is a key focus of our research. Whereas ISO/IEC 38500 takes a behavioral stance, offering guidance about governance behavior, COBIT 5 takes a process stance, offering guidance about process, mainly suggesting auditable performance metrics rather than process descriptions.

Process-oriented IT management frameworks, including processes for extended aspects of management dealing with the business use of IT, are frequently important, especially in larger organizations, but are insufficient to guarantee good governance and management because they are at risk of poor behavior by individu-

als and groups within and sometimes even external to the organization. The best process model is often readily defeated by poor human behavior. We see evidence of poor behavior in many investigations of failed IT projects (such as the Queensland Audit Office 2009 review of Queensland Health Payroll[11]). On the other hand, good behavior ensures conformance with an effective process model and compensates for deficiencies in weaker process models.

In any effective approach to the governance of IT, the main activities described in ISO/IEC 38500—direct, evaluate, monitor—must be performed following the six principles of this standard and must guide behavior with respect to IT management.

Good corporate governance is not the only reason for organizations to improve governance of IT. From the outset, most discussions identify "stakeholder value drivers" as the main reason for organizations to upgrade governance of IT. Stakeholder pressure drives the need for effective governance of IT in commercial organizations. Lack of such pressure may explain why some public services have less effective governance of IT.[12] The framework depicted in Weill and Ross[14] has been expanded for governance of IT (see Figure 3), showing the connection between corporate governance and key-assets governance.

Figure 3 emphasizes the system for governance of IT extends beyond the narrow domain of IT-management processes. The board's relationships are outlined at the top of the framework. The senior executive team is commissioned by the board to help it formulate strategies and desirable behaviors for the organization, then implement the strategies and behaviors. Six key asset classes are identified below the strategy and desirable behaviors. In this framework, governance of IT includes specifying the decision rights and accountability framework responsibilities (as described in ISO/IEC 38500) to encourage desirable behavior in the use of IT. These responsibilities apply broadly throughout the organization, not only to the CIO and the IT department. Governance of IT is not conceptually different from governing other assets (such as financial, personnel, and intellectual property). Strategy, policies, and accountability thus represent the pillars of the organization's approach to governance of IT.

This behavioral approach is less influenced by and less dependent on processes. It is conducted through decisions of governance structures and proper communication and is much more focused on human communities and behaviors than has been proposed by any process-oriented IT management model.

Conclusion

Focusing on technology rather than on its use has yielded a culture in which business leaders resist involvement in leadership of the IT agenda. This culture is starkly evident in many analyses of IT failure. Business leaders have frequently excused themselves from a core responsibility to drive the agenda for business performance and capability through the use of all available resources, including IT.

Governance of IT involves evaluating and directing the use of IT to support the organization and monitoring this use to achieve business value. As defined in ISO/IEC 38500, governance of IT drives the IT management framework, requiring top-down focus on producing value through effective use of IT and an approach to governance of IT that engages business leaders in appropriate behavior. Governance of IT includes business strategy as the principle agenda for the use of IT, plus the policies that drive appropriate behavior, clear accountability and responsibility for all stakeholders, and recognition of the interests and behaviors of stakeholders beyond the control of the organization.

Using ISO/IEC 38500 to guide governance of IT, regardless of which models are used for management systems, ensures governance of IT has appropriate engagement of the governing body, with clear delegation of responsibility and associated accountability. It also provides essential decoupling of governance oversight from management detail while preserving the ability of the governing body to give direction and monitor performance.

Asking whether to govern IT, or not to govern IT should no longer be a question. Governing IT from the top, focusing on business capability, performance, and value should be normal behavior in any organization, generating business value from investment in and the ongoing operation of IT-enabled business capability, with appropriate accountability for all stakeholders.

Acknowledgment

This work was partially supported by the Spanish Ministry of Economy and Competitiveness under grant TIN2011-23889. C

References

1. Cadbury, A. (chair). *Report of the Committee on the Financial Aspects of Corporate Governance.* Burgess Science Press, London, U.K., 1992.
2. de Haes, S. and Van Grembergen, W. IT governance and its mechanisms. *Information Systems Control Journal 1* (2004), 1–7.
3. ISO/IEC. *ISO/IEC 38500: 2008 Corporate Governance of Information Technology.* ISO/IEC, Geneva, Switzerland, June 2008; http://www.iso.org/iso/catalogue_detail?csnumber=51639
4. IT Governance Institute. *Board Briefing on IT Governance, Second Edition.* IT Governance Institute, Rolling Meadows, IL, 2003; http://www.isaca.org/restricted/Documents/26904_Board_Briefing_final.pdf
5. Juiz, C. New engagement model of IT governance and IT management for the communication of the IT value at enterprises. Chapter in *Digital Enterprise and Information Systems*, E. Ariwa and E. El-Qawasmeh, Eds. *Communications in Computer and Information Science Series, Vol. 194.* Springer, 2011, 129–143.
6. Juiz, C., Guerrero, C., and Lera, I. Implementing good governance principles for the public sector in information technology governance frameworks. *Open Journal of Accounting 3*, 1 (Jan. 2014), 9–27.
7. Juiz, C. and de Pous, V. Cloud computing: IT governance, legal, and public-policy aspects. Chapter in *Organizational, Legal, and Technological Dimensions of Information System Administration*, I. Portela and F. Almeida, Eds. IGI Global, Hershey, PA, 2013, 139–166.
8. Langland, A. (chair). *Good Governance Standard for Public Services.* Office for Public Management Ltd. and Chartered Institute of Public Finance and Accountancy, London, U.K., 2004; http://www.cipfa.org/-/media/Files/Publications/Reports/governance_standard.pdf
9. Professional Accountants in Business Committee of the International Federation of Accountants. *International Framework, Good Governance in the Public Sector: Comparison of Principles.* IFAC, New York, 2014; http://www.ifac.org/sites/default/files/publications/files/Comparison-of-Principles.pdf
10. Stachtchenko. P. Taking governance forward. *Information Systems Control Journal 6* (2008), 1–2.
11. Toomey, M. Another governance catastrophe. *The Infonomics Letter* (June 2010), 1–5.
12. Toomey, M. *Waltzing With the Elephant: A Comprehensive Guide to Directing and Controlling Information Technology.* Infonomics Pty Ltd., Victoria, Australia, 2009.
13. Van Grembergen, W. *Strategies for Information Technology Governance.* Idea Group Publishing, Hershey, PA, 2004.
14. Weill, P. and Ross, J.W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results.* Harvard Business School Press, Cambridge, MA, 2004.

Carlos Juiz (cjuiz@uib.es) is an associate professor at the University of the Balearic Islands, Palma de Mallorca, Spain, and leads the Governance of IT Working Group at AENOR, the Spanish body in ISO/IEC.

Mark Toomey (mtoomey@infonomics.com.au) is managing director at Infonomics Pty Ltd., Melbourne, Australia, and was the original ISO project editor of ISO/IEC 38500.