Use of Information Technology has matured enough to require top level governance in addition to established disciplines for management and operation

BY CARLOS JUIZ AND MARK TOOMEY

To Govern IT or not to Govern IT

Business leaders bemoan the pains of governing IT but the alternative might be still worse

Key Insights

- Governance of IT is a board and top executive responsibility that must focus on business performance and capability, rather than technology details.
- Major business transformations, enabled by new technology, are taking place in established organisations: these require top-down focus on business strategy, capability and performance through effective use of IT, and an approach to Governance of IT that engages business leaders in appropriate behavior.
- A principles-based approach to Governance of IT, as described in ISO/IEC 38500, is consistent with broader models for guidance on governance of organisations, and is accessible to business leaders who have no specific technology skills.
- Adoption of ISO/IEC 38500 to guide Governance of IT provides rich engagement of leaders in planning, building and running the IT-enabled organization, and enables directors and senior executives to be appropriately diligent in their duties to direct and control the organizaton's use of IT.

To govern or not govern Information Technology (IT) is no longer a choice for any organization. Information Technology is a major instrument of business change in private and public sector businesses. Without good governance, organizations face loss of opportunity and potential failure. Effective Governance of IT promotes achievement of business objectives but poor Governance of IT obstructs and limits this achievement.

The need to govern IT comes from two factors: business necessity and enterprise maturity. Business necessity arises because many actors in the market use technology to gain advantage. Consequently, remaining relevant and competitive requires organizations to deeply integrate the IT agenda and business strategic plans, to ensure appropriate positioning of technology opportunity and appropriate response to technology enabled changes in the marketplace. Enterprise maturity arises because a narrow focus on operating infrastructure, architecture and service management of an owned IT asset is no longer key to development of the organization.

Achieving value involves more diverse arrangements for sourcing, ownership and control arrangements, in which use of IT assets is also not linked to direct administration of IT assets. Increasingly, divestment activities create unintended barriers to flexibility as mature organizations respond to new technology enabled pressures. Paradoxically, contemporary sourcing options, such as cloud computing and software-as-a-service, are developments that can increase flexibility and responsiveness. Thus it can be seen that the two factors, business necessity and enterprise maturity, overlap and feed one to the other.

The International Standard for Corporate Governance of Information Technology, ISO/IEC 38500 [14], was developed by experts from government and industry who understood at a deep intuitive level the critical importance of resetting the focus for Governance of IT on business issues, without losing sight of the technology issues. While it doesn't say so explicitly, careful consideration of the guidance in the standard leads to one inescapable, three part conclusion, that business leaders must take up primary responsibility for:

- setting the agenda for use of IT as an integral aspect of business strategy;
- successful delivery of investments in IT-enabled business capability;
- ongoing successful operational use of IT in routine business activity.

Additionally, implementation of effective arrangements for Governance of IT should answer the need for organizations to ensure value creation from investments in IT. Without good Governance of IT, there is risk of inappropriate investment, failure of services and non-compliance to regulations.

Using the terminology in [8]; proper Governance of IT is needed to ensure that investments in IT generate required business value and that risks associated with IT are mitigated. This latest consideration to value and risk are closer to the principles of good governance, but there remains in management-based 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 1990's, and diverse definitions have emerged for IT Governance. 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, through selection and delivery of IT projects and on to the operational aspects of IT systems. Such definitions and models should have improved the capability of organizations to ensure that their IT activities remain on track to achieve their strategies and goals. They should also have provided ways to measure IT performance, so that IT Governance should answer questions regarding how the IT department is functioning and generating return on investments for the business.

Understanding that older definitions and models for IT governance have focused on 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 regarding what exactly is governance and management (and even operation) of IT. The reason for this misunderstanding was because the frontiers between both may be somewhat diluted and by a propensity of the IT industry to inappropriately refer to management activities as IT Governance [2].

There is widespread recognition that IT is not a stand-alone business resource. IT only delivers value when it is used effectively to enable business capability and to open opportunities for new business models. What were previously seen as IT activities should be viewed as business activities that embrace use of IT. Thus, Governance of IT must 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 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.

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

The term Governance of IT is equivalent to the terms Corporate Governance of IT, Enterprise Governance of IT and Organizational Governance of IT. In any case, 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 achievement of the organization's purpose and objectives, and conformance [9] of 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 at enterprises do not match. Conflicts of interest between owners (shareholders), managers and other stakeholders (citizens, clients or users) can occur whenever these roles are separated. Corporate governance includes development of mechanisms to control actions taken by the organization and safeguard the stakeholders' interests as appropriate [4]. Private and Public organizations today are subject to many regulations governing data retention, confidential information, financial accountability and recovery from disasters. While no regulations require a Governance of IT framework, many have found it to be an excellent way to ensure regulatory compliance [6]. By implementing effective Governance of IT, organizations establish internal controls needed to meet core guidelines of many regulations.

Some IT specialists mistakenly think that business leaders cannot govern IT, since they don't have technology skills. To understand the capability that Information Technology brings, or to

plan new and improved business capability enabled by smarter, more effective and innovative 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 motor car: one does not need to be a designer or a manufacturing engineer to operate a taxi service – but one does need to understand the capabilities and service requirements for vehicles used to operate the taxi 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 description of management systems and processes. In common with many broader guides for corporate governance and governance in the public sector, AS 8015 used a principles-based approach, and focused its guidance on business use of IT and business outcomes, rather than on the technical supply of IT. ISO/IEC 38500, issued in 2008, is evolved from AS 8015 and is the first international standard that provides guidelines for Governance of IT. In fact, the selection of 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 [12].

As mentioned above, since well before release of either AS 8015 or ISO/IEC 38500, many organizations have confused governance and management of IT. The confusion has been exacerbated by efforts to integrate some aspects of governance in common de facto standards for IT Management, resulting in these governance aspects being described in management systems terms. In an effort to eliminate confusion, we will 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. Figure 1 shows the main standards for Governance of IT and IT Management.

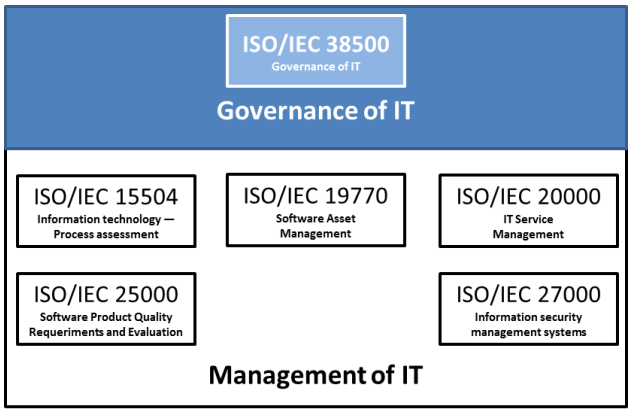

Figure 1. Main ISO/IEC Standards of Governance and Management

Figure 2 depicts the latest draft 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, Toomey [2] has presented evolved versions of the original ISO/IEC

38500 model, which convey more clearly the distinction between governance and management activities and the business orientation essential for effective use of IT from the governance viewpoint. In figure 2, we now integrate Toomey's and the ISO/IEC 38500 newer 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 delegation may 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, exactly as occurs in respect of finance and human resources. There is an implicit expectation that the governing body will require management to establish management systems to plan, build and run the IT-enabled organization.

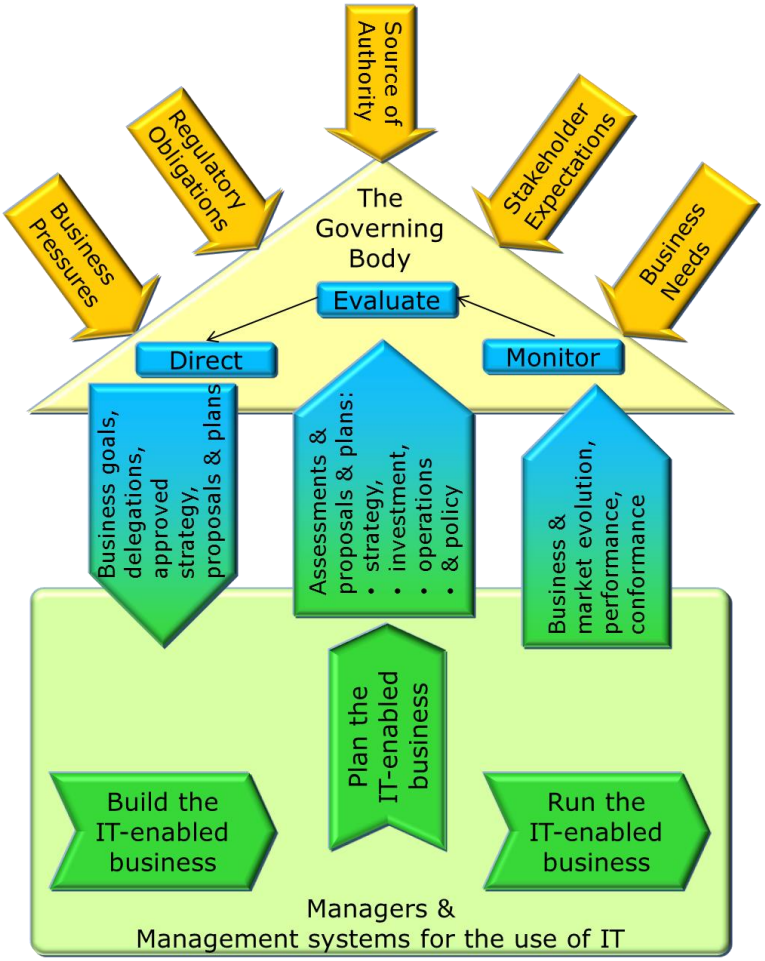

Figure 2. Model for Governance of IT elaborated from current DIS ISO/IEC 38500.

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

- 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* use of IT with regard to *business and marketplace evolution*.
- Business and IT units collaboratively develop *Assessments Proposals and plans* for business strategy, investments, operations and policy that through activities to *plan the IT-enabled business*.
- The Governing Body *evaluates* the proposed *Assessments Proposals and Plans* and, where appropriate, *directs* that these be adopted and implemented. The governing body then *monitors* that implementation of the plans and policies are delivering required *performance and conformance*.

Within the management space:

- 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 use of IT and for investment in IT-enabled business capability.
- Investment in projects to *Build the IT-enabled business* are undertaken as *directed* by and in conformance with delegations, plans, policies approved by the board. Project personnel with business change and technology skills work with line managers to build IT-enabled business capability.
- To close the virtuous cycle, once the projects become a reality, they deliver the capability to *Run the IT-enabled business* the business, supported by appropriate management systems for the operational use of IT.
- All activities and systems involved in planning, building and running the IT-enabled business are subject to ongoing *monitoring* of evolving market conditions, performance against expectations and conformance to internal rules and external norms, as appropriate.

ISO/IEC 38500 sets out six principles for good corporate Governance of IT that express preferred behavior to guide decision making. By merging and clarifying the titles for the principles from AS 8015 and ISO/IEC 38500, we derive a clear summary of these principles:

1. Responsibility: Establish clearly understood (and appropriate) responsibilities for (decisions relating to use and supply of) IT;
2. Strategy: Plan (supply and use of) IT to best support the organization;
3. Acquisition: Invest (in new and ongoing use of IT) validly;
4. Performance: Ensure that IT performs well (in respect of business needs), whenever required;
5. Conformance: Ensure (all aspects of decision making, use and supply of) IT conforms with formal rules;
6. Human behavior: Ensure (planning, supply and use of) IT respects human behavior.

These principles and activities clarify the behavior expected through implementing Governance of IT, as Stachtchenko stated in [10]:

- Stakeholders delegate accountability and stewardship to the governance body and, in exchange, expect the governance body to assume accountability for activities necessary to meet expectations.
- The governance body sets direction for management of the organization and holds management accountable for overall performance.
- The governance body takes a stewardship role, in its traditional sense of assuming responsibility for management of something entrusted to one's care.

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

Van Grembergen [7] 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 and in this way ensure fusion of business with IT. It consists of leadership, organizational structures, and processes that ensure that the organization's IT sustains and extends the organizational strategy and objectives. This definition is loosely consistent with ITGI's [3] definition that Governance of IT is a part of enterprise governance that consist of leadership, organizational structures, communication mechanisms and processes that ensure that 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 both, while embracing the notion that effective governance depends on effective management systems, tend to focus on the system aspects rather than the true governance aspects.

According to Weill & Ross [1], Governance of IT involves specifying the decision rights and accountability framework to produce desired behavior in the use of IT at the organization. Van Grembergen asserts that Governance of IT is the responsibility of executives and senior management that consists of leadership, organizational structures and processes that ensure that IT assets are supporting and extending the company objectives and strategies of the organization. By focusing on how decisions are made underscores the first of the ISO/IEC 38500 principles, emphasizing that behavior in assignment and discharge of responsibility are critical to deriving value from investment in IT and to overall organization performance.

Thus, Governance of IT must include a framework for organization-wide decision rights and accountability to encourage desirable behavior in the use of IT. Within the broader system for Governance of IT, IT Management just focuses on a small but critical set of IT-related decisions: IT principles, enterprise architecture, IT infrastructure capabilities, business application needs, and IT investment and prioritization [1]. Even though essential to govern IT and its core is deeply behavioral, this is a definition of the implementation framework of IT-related decisions. These decision rights define mainly who makes decisions delegated by the

governing body, and what are they deciding (and the way they are doing it). Focusing on decision rights intrinsically defines behavioral rather than process aspects for Governance of IT.

Similarly, process-oriented IT Management as described in COBIT and similar frameworks is also a part of the governance of IT, ensuring that IT activities support and enable the 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 into broader issues of setting business strategy which is now influenced by, as well as setting the agenda for the use of IT. Nor do they extend fully into the realms of business capability development and operational management that are intrinsic to the use of IT in most organizations. The latest version of COBIT (COBIT 5) included for the first time the ISO/IEC 38500 model. However, there is a quite fundamental and significant difference between ISO/IEC 38500 and COBIT 5, which is a key focus for our research. Whereas ISO/IEC 38500 has a behavioral stance – offering guidance about behavior, COBIT 5 has 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 dealing with 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 individuals and groups within and sometimes external to the organization. We assert that the best model can be readily defeated by poor behavior. We see evidence of poor behavior in many investigations of failed IT projects, such as the Queensland Audit Office review of Queensland Health Payroll [13]. On the other hand, good behavior directly nature ensures conformance to an effective process model and compensates for deficiencies in weaker process models.

Thus, in an effective approach to Governance of IT, the main activities described in ISO/IEC 38500: direct; evaluate; and monitor; must be performed following the six principles, and these principles must guide behavior in respect of IT Management.

Good corporate governance is not the unique reason for organizations to improve Governance of IT. From the outset, most discussions of the subject identify the '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. Absence of such pressures may explain why some public services have less effective Governance of IT [11]. The framework depicted in [1] has been expanded for Governance of IT (see figure 3) and illustrates the connection between corporate governance and key asset governance.

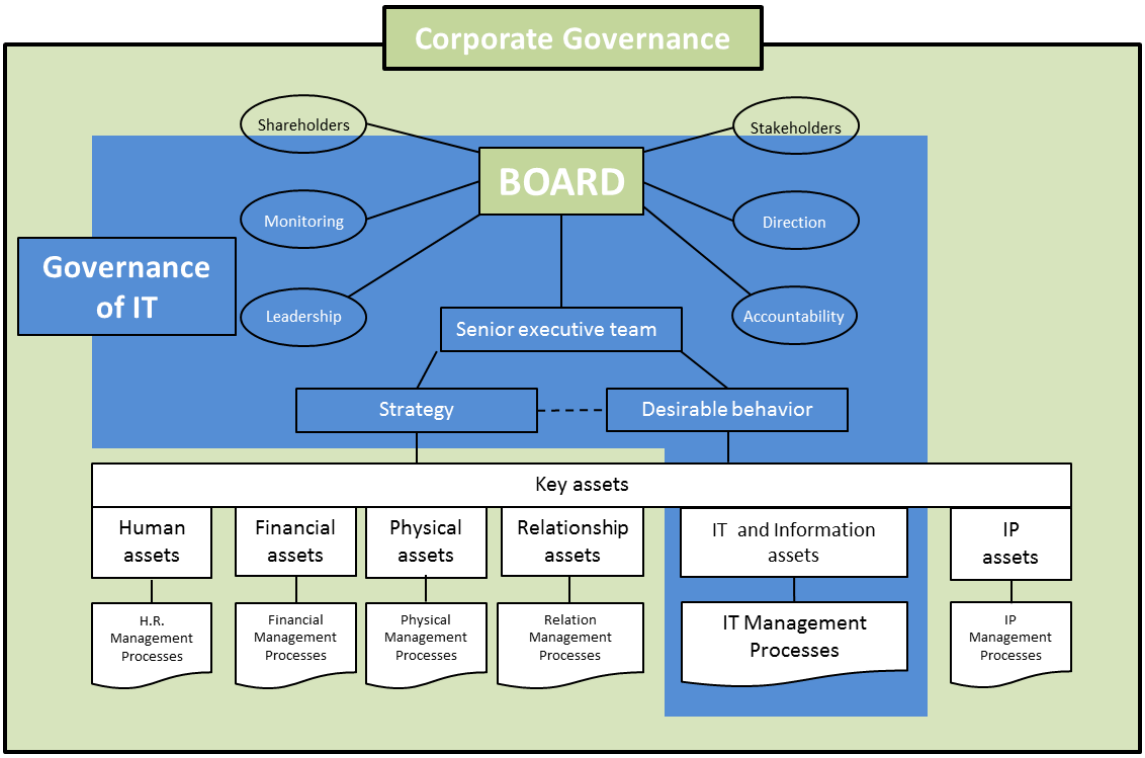

Figure 3. Coverage area for behavior-oriented Governance of IT and IT Management, linking corporate and key assets (own elaboration from [1]).

Figure 3 emphasizes that the system for Governance of IT extends beyond the narrow space of the IT Management processes. At the top of the framework, the board's relationships are shown. The senior executive team is commissioned by the board to help the board formulate strategies and desirable behaviors for the organization, and then to implement those strategies and behaviors. Below the strategy and desirable behaviors, six key asset classes are identified. 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 use of IT. These apply broadly throughout the organization: not only to the CIO and the IT department. Governance of IT is not conceptually different of governing other assets, such as financial, personnel, intellectual property, etc. Thus, the strategy, policies and accountabilities form the pillars of the organization's approach to Governance of IT.

This behavioral approach to the Governance of IT is less influenced by and less dependent on processes. It is conducted by decisions of governance structures and proper communication and is much more focused on human communities and behaviors than is proposed by any process-oriented IT Management models.

Conclusion

Focusing on technology rather than its use has enabled development of a culture in which business leaders resist involvement in leadership of the IT agenda. This culture is starkly evident in many reviews of IT failures. Business leaders have frequently absented and excused themselves from a core responsibility to drive the agenda for business performance and capability through effective 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. We see that Governance of IT, as defined in ISO/IEC 38500, drives the IT management framework. This requires top-down focus on getting value through effective use of IT and an approach to Governance of IT that engages business leaders in appropriate behavior. Governance of IT includes the business strategy as the principle agenda for 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 who lie beyond the control of the organization.

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

Thus, to govern IT or to not govern IT should not be a question anymore. To govern 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 ongoing operation of IT-enabled business capability, with appropriate accountability to all stakeholders.

Acknowledgements

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

References

[1] P. Weill and J.W. Ross. IT Governance: How Top Performers Manage IT Decision Rights for Superior Results, Harvard Business School Press, 2004.

[2] M. Toomey. Waltzing with the Elephant: A comprehensive guide to directing and controlling information technology, Infonomics Pty Ltd., 2009.

[3] Board Briefing on IT Governance, 2nd Edition. IT Governance Institute, 2009, http://www.itgi.org/.

[4] OPM, and CIPFA. Good Governance Standard for Public Services, 2004.

[5] C. Juiz. “New Engagement Model of IT Governance and IT Management for the Communication of the IT Value at Enterprises”, DEIS 2011: 129-143, 2011.

[6] IFAC. Comparison of Principles, 2013, http://www.ifac.org/sites/default/files/publications/files/Comparison-of-Principles.pdf.

[7] W. Van Grembergen. Strategies for Information Technology Governance, IGI, 2003.

[8] S. de Haes and W. Van Grembergen. “IT Governance and Its Mechanisms”, 2004, http://www.isaca.org/Journal/Past-Issues/2004/Volume-1/Documents/jpdf041-ITGovernanceandIts.pdf.

[9] C. Juiz, and V. de Pous. “Cloud Computing: IT Governance, Legal, and Public Policy Aspects”, in Organizational, Legal, and Technological Dimensions of Information System Administration (Portela and Almeida, eds.), pp. 139-166, 2013.

[10] P. Stachtchenko. “Taking Governance Forward”, 2008, http://www.isaca.org/Journal/Past-Issues/2008/Volume-6/Documents/jpdf0806-taking-gov-forward.pdf.

[11] C. Juiz, C. Guerrero, and I. Lera, "Implementing Good Governance Principles for the Public Sector in Information Technology Governance Frameworks," *Open Journal of Accounting*, Vol. 3 No. 1, 2014, pp. 9-27.

[12] Report of the Committee on the Financial Aspects of Corporate Governance. (Chair: Sir Adrian Cadbury), Burgess Science Press, London, 1992.

[13] M. Toomey. Another Governance Catastrophe, in The Infonomics Letter June 2010 Edition. Infonomics Pty Ltd, June 2010. http://www.infonomics.com.au/Web%20Content/Documents/The_Infonomics_Letter_June_2010.pdf

[14] ISO/IEC 38500, International Standard for Corporate Governance of IT, 2008.

Biographies

Carlos Juiz (cjuiz@uib.es) is ACM Senior Member and Associate Professor at University of the Balearic Islands, Palma de Mallorca, Spain. He 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. He was the original ISO Project Editor for ISO/IEC 38500 and is an international authority on its use.