

GUEST EDITORIAL

Research on IT Governance, Risk, and Value: Challenges and Opportunities

I. INTRODUCTION

This theme issue of the *Journal of Information Systems* sees the publication of seven papers that cover a variety of facets of research on the governance of information technology. IT governance (ITG) is the process by which organizations seek to ensure that their investment in information technology facilitates strategic and tactical goals. IT governance is a subset of broader corporate governance, focusing on the role played by information technology within the organization. There are several important dimensions of ITG. Arguably the most important element of ITG is the design of decision rights and organizational structures. What role do governing bodies, such as the Board of Directors, play in the oversight and direction of IT? What roles and responsibilities for IT does the governing body assume and what is delegated to senior and operational management? How is IT to be structured within the organization? Is the provision of IT to be centrally organized within a single, functional IT organizational unit? Or, perhaps, is provision of IT to be largely distributed to operational or administrative units within the organization? Other dimensions of ITG, as noted by [Wilkin and Chenhall \(2010\)](#), include strategic alignment between organizational goals and needs and IT outcomes; management of risk; value delivery; and measurement of performance.

ITG has become more important within organizations as the important role that IT plays in adding organizational value has become increasingly clear ([Brynjolfsson and Saunders 2010](#); [Masli et al. 2011](#); [Tambe and Hitt 2012](#)). Investment in IT is a significant proportion of current and capital spending in most industries, giving additional impetus to ITG. IT is also subject to high levels of environmental instability. How are organizations to respond to the insourcing/outourcing nexus, cloud computing, virtualization, and mobile computing among other environmental challenges? Equally, the compliance requirements arising from overall (e.g., SOX) and industry (e.g., HIPAA, Basel II, PCI) regulatory regimes have given an added impetus to ITG efforts. Given that IT both mitigates risk (e.g., by supporting internal control processes) and creates risk (e.g., by exposure of corporate IT systems to external threats), there is an increased understanding that IT is an important component of enterprise risk management ([Parent and Reich 2009](#); [Wilkin and Chenhall 2010](#)). While these challenges are compelling for many organizations and particularly for governing bodies, they are shared by a wide variety of organizations. While there may be entity, industry, or national differences, all entities must address questions such as “how is IT to be organized?” or “how much of the provision of IT should we move to cloud providers?” There are also many aspects of IT provision (e.g., security, enterprise architecture, user management, software

development) that transcend industry differences. As a result, the ITG domain is quite well served by guidance and governance frameworks designed to provide structure and good practice that organizations can adopt and adapt. These include ISO 38500 and COBIT (ISACA 2012; ISO/IEC 2008). These organizing frameworks provide a foundation by which ITG can be understood and measured at national, industry, and entity levels. At the same time, these frameworks are themselves potential objects for research in ITG.

ITG is increasingly systematically adopted, particularly by larger organizations. A recent international survey by ISACA shows that more than 70 percent of organizations with less than 500 full-time employee equivalents (FTEs) and 85 percent of organizations with more 500 FTEs report that they have some ITG processes in place (ISACA 2011). The ISACA study shows that overall maturity of ITG processes is still relatively low, especially given that the survey was self-reported.

In summary, then, ITG is an important area for both the practice and research domains. Importantly for the community served by the *Journal of Information Systems*, many of the long-standing concerns of the accounting information systems (AIS) research community correlate closely with the various dimensions of ITG. There is strong evidence of this relationship in the literature review by Wilkin and Chenhall (2010), published recently in the *Journal of Information Systems*. For example, the research conducted in AIS on information assurance is highly relevant to several dimensions of ITG including risk management and performance measurement (Boritz 2002; Boritz 2005; Boritz and Hunton 2002; Wright and Wright 2002). Other areas of research that are important in the AIS domain and that impact on ITG include IT internal controls, value realization from IT investment, ERP systems, IT audit, continuous monitoring, and business process management to pick just a few. Indeed, 41 of the 496 papers (8 percent) analyzed by Wilkin and Chenhall (2010) were from *JIS* and the *International Journal of Accounting Information Systems (IJ AIS)*. The papers from *JIS* and *IJAIS* referenced by Wilkin and Chenhall (2010) encompass all of the dimensions of ITG. A further 109 papers (21 percent) are drawn from *Accounting, Organizations and Society* and *Management Accounting Research*, primarily focused, as might be expected, on the performance measurement domain. I expect that while researchers in AIS may not necessarily “own” the ITG research domain, we will be recognized as core contributors to research on ITG. Hence, this theme issue of the *Journal of Information Systems* seeks to reinforce the link between AIS and research on IT governance, risk, and value. In this editorial, I review the research questions canvassed in the theme issue and set out some opinions on the nexus between research on ITG and AIS.

II. THEME ISSUE: IT GOVERNANCE, RISK, AND VALUE

This theme issue on IT governance, risk, and value arose from traditions in AIS research and as a natural extension to the research synthesized in Wilkin and Chenhall (2010). The call for papers reflected the wide range of research interests within the ITG domain. In particular, the call emphasized more recent concerns with areas such as value management, value delivery, risk management, and integration of ITG with corporate governance. There are seven papers in the theme issue. Thanks to the efforts put in by the authors and an impressive and hard-working group of reviewers drawn internationally from the AIS and MIS domains, the theme issue was completed in less than a year. The papers traverse the complete range of research dimensions within ITG.

A core dimension of ITG is strategic alignment between the information technology function and other functions (“the business”) in the organization. Much of the research on strategic alignment revolves around involvement of the business in strategic planning (e.g., Chen et al. 2008; Tallon 2007; Tallon and Pinsonneault 2011); setting technological directions (e.g., Ravishankar et al. 2011); project initiation, direction and management (e.g., Velcu 2010); and impact of strategic alignment on firm performance (e.g., Cragg et al. 2002; Fink and Neumann 2009). Schobel and

Denford (2013) take a somewhat different perspective on strategic alignment. They investigate the CIO/CFO dyad, an under-researched relationship. Intuitively this dyad seems important for the success of IT. The CFO is a major consumer of IT services. The CFO is typically involved in strategic and tactical decision making for a wide range of entity-level and functional issues. Further, given that the foundations of business processing often arose from the finance function, in many organizations the CFO was responsible for IT. In some organizations, the CIO reports to the CFO. Clearly, this dyad is important. Schobel and Denford (2013) address various facets of the CIO/CFO relationship including ongoing engagement, personal considerations, and the nature of the CIO and CFO roles within the organization. They analyze the impact of these factors on strategic alignment effectiveness. Schobel and Denford (2013) adopt a case study approach, which is appropriate given the paucity of research in the area and the early stage of theory development. The results for the three case studies show that “trust and shared understanding appeared to be the key contributors to an effective relationship.”

Ali et al. (2013) address the issue of the level of knowledge on ITG held by the top management team (TMT) and the ability of the TMT to turn this knowledge into competitive advantage. The authors adopt and adapt constructs in the literature for knowledge “adaptive capacity” to the ITG domain. What knowledge does the TMT have about ITG? How is this knowledge communicated within the TMT? How does the TMT undertake environmental scanning on ITG? In a survey of members of TMTs in Australian private-sector entities, they associate these factors with the “absorptive capacity” of ITG (i.e., ITG implementation outcomes). Ali et al. (2013) find that prior ITG knowledge and the quality of inter-TMT communication are most strongly associated with ITG outcomes. Interestingly, the authors go on to establish a strong association between ITG absorptive capacity with entity efficiency and growth vectors.

Prasad et al. (2013) view ITG through an inter-organizational lens. This lens is particularly important given the increased integration of value chains. Increasingly, organizations are dependent on partners and the integration of inter-organizational information systems up and down the value chain. The authors focus on relational mechanisms designed to better align the performance of the partners. In a survey of entities that have significant value chain partners, Prasad and Green (2013) find that the existence and quality of partner relational mechanisms, including steering committees and performance measurement systems, are strongly associated with the business value arising from the partnership.

Close to the research interests of many in the AIS community, Héroux and Fortin (2013) study the relationship between the internal audit function and ITG outcomes. At a prescriptive level, it is clear that the internal audit function should play an important role in managing risk and providing feedback on IT efficiency and effectiveness. Whether this happens in practice is an entirely different matter. Héroux and Fortin (2013), employing survey methodology, study whether internal audit resources, competencies, and interaction with the governing board influence the internal audit function’s involvement in ITG. The authors find that, for the organizations surveyed, the level of resources devoted to IT audit was typically low. The involvement of internal audit in ITG was primarily at the process level, particularly from a risk management perspective. There was little evidence of internal audit involvement in ITG structures or relational mechanisms.

As the Internet has become pervasive and fundamental to value-adding processes in a wide range of organizations, information security has become central to the IT mission. Breaches of information security may, for larger for-profit entities, make a clear impact on stock valuation in capital markets, (Chai et al. 2011; Gordon et al. 2010). Kwon et al. (2013) investigate the relationship between the key characteristics of senior IT executives, including involvement in the top management team (TMT), and compensation, and the level of information security breaches. Kwon et al. (2013) assert that these characteristics are tangible outcomes of IT governance decisions. The authors find that involvement in the TMT and what they term “behavior-based

compensation” (i.e., salary) is negatively associated with subsequent security breaches. They do not find such a relationship for “outcome-based compensation.” In essence, [Kwon et al. \(2013\)](#) provide empirical support for the assertion that more mature ITG processes mitigate security risks.

As I note above, the ITG domain features a number of governance frameworks. These are designed to provide organizations with structures and good practice statements that allow them to enhance their ITG performance. These frameworks include ISO 38500 and COBIT. There are a number of other frameworks at the governance layer, including COSO, and at the operational layer, such as ITIL. The COBIT framework, now in its fifth iteration, is an influential ITG framework. COBIT is designed to provide structure for governance decision making across the complete lifecycle of investment in information technology. COBIT 5, while building on the foundation of earlier versions (e.g., domains, business processes, maturity models, RACI charts), makes some significant changes in design and implementation. There are, for example, markedly enhanced mechanisms for aligning organizational goals with IT goals and IT delivery. While the role of organizational units outside of IT was recognized in earlier versions, COBIT 5 explicitly reflects the reality that responsibility for the success of IT rests with both IT functions and other support and operational units. [De Haes et al. \(2013\)](#) provide an overview of the design imperatives in COBIT 5. They describe a set of research opportunities that would both see COBIT 5 as the unit of analysis and as an organizing resource. The research opportunities set out by [De Haes et al. \(2013\)](#) correlate with those outlined by [Janvrin et al. \(2012\)](#) on the COSO internal control framework.

An important ingredient of ITG is the level of process maturity. The ability of organizations to leverage information technology for value generation and management of risk depends in large measure on the maturity and reliability of a myriad of business processes, organizational structures, and relational mechanisms. Formalized mechanisms to measure process maturity have been a feature of the software development world for decades (e.g., CMM, CMMI). [Debreceeny and Gray \(2013\)](#) undertake a large field study to measure the process maturity of IT business processes at the governance and managerial layers. They use the business processes in COBIT 4 as a foundation for their study. They interact with process owners at 52 organizations in several countries to measure process maturity. The authors apply an extensive survey instrument on ITG characteristics in face-to-face interviews with the CIO. [Debreceeny and Gray \(2013\)](#) find that the mean level of process maturity is rather low, with higher process maturity being observed in more operational and established processes. They find that the level of business/IT alignment is the most significant predictor of the level of process maturity.

III. FUTURE RESEARCH DIRECTIONS

ITG research is in an interesting state. Some aspects of ITG are well explored. For example, the research on business/IT alignment is long standing and well established. There is very little comparative advantage to be exploited by additional research. There are, however, other facets of ITG research where very little is known. For example, the study by [Debreceeny and Gray \(2013\)](#) on process maturity is one of only a handful of papers that systematically address the level of process maturity for a range of organizations. There is a clear need for additional research in this area. Further, connecting process maturity to strategic and tactical priorities is even more difficult. What level of process maturity should an entity desire? What should govern these decisions? How do stakeholders at the governance and management layers decide on appropriate levels of process maturity? What are the returns from process improvement? Indeed, what are the returns from investment in ITG itself? How does ITG maturity correlate with key entity-level metrics (e.g., cost efficiency, agility, reliability)? In this issue, [Ali et al. \(2013\)](#) provide some evidence of how top-management team knowledge is associated with efficiency and strategic growth. There is much more yet to learn about these relationships. Similarly, research on the nexus between ITG and value

generation from IT investment is highly limited. While there is extensive, growing, and welcome research on the effect of IT investment on firm performance, there is very little research on the governance and management processes that give rise to superior returns at the level of the entity.

When we conduct research in a number of aspects of AIS, we should consider how the research fits within a broader IT governance perspective. For example, as I note above, the internal audit function and particularly IT audit should play a key feedback and performance enhancement role in ITG. Yet many aspects of research in internal audit seem rather functional in nature. ITG is multifaceted. Putting processes in place at any organization that covers even a fraction of what is encompassed in, for example, COBIT 5 is highly challenging. Understanding the existence, design, and effectiveness of ITG processes is significantly more challenging and yet more important than, for example, running audits of change management or user management, or even continuous monitoring of the state of transactional databases. Similar challenges could be made for research in areas such as internal control and ERP systems.

Successful adoption of ITG is challenging and we know very little about what constitutes a successful path to ITG. There are many moving parts in ITG involving governing bodies (e.g., the Board of Directors and the Audit Committee), operational management, and the IT function and business partners. Consider the case of business/IT alignment. Much of the existing business/IT alignment literature is built upon rather prosaic assumptions. The literature typically sees the IT function as being the primary delivery agent and responding to demands from operational management. This view of the relationship between IT and operational management has become outdated as the loci of IT production has become significantly more dispersed in recent years. Decisions on how IT is to be prioritized and administered require the significant participation of operational management. Business/IT alignment is not unidirectional. Rather, it requires integration of the objectives and organizational outcomes of operational and IT management. This perspective of shared responsibility for IT direction and outcomes is often challenging for both operational and IT management. Often, for example, operational management will take the perspective that for any solution for organizational imperatives that involves IT, responsibility will lie with the IT function—when in fact responsibility should be shared. How these tensions impact successful ITG adoption gives rise to interesting and important research questions.

Changes in the technological environment present many challenges to ITG with resulting research opportunities. For example, security and cloud computing play increasingly important roles in the IT environment. Operational management can now draw on cloud-based services to meet their tactical needs, without necessarily even involving the IT function. This is not a repeat of the end-user computing debate of the 1980s and 1990s, which was at the periphery of organizational computing. Rather, core functions can be implemented by operational management. These technological changes do not necessarily give rise to new forms of ITG. There should not be “security governance” or “cloud governance,” as distinct from ITG, more generally. Rather ITG and research, thereon, must respond to these changes in the environment.

An interesting outcome of the research analyzed by [Wilkin and Chenhall \(2010\)](#) is the significant contribution made by researchers in the management accounting community. Very few of these papers were explicitly designed to address ITG, *per se*. Rather, research on questions such as the design of performance measurement systems, application of balanced scorecard techniques, and investment program management all have direct application for research on ITG. It is clearly time for AIS researchers to reach out and work with their colleagues in management accounting to design research projects in ITG that exploit the relevant comparative advantage of AIS researchers in areas such as IT, internal controls, and IT audit and the comparative advantage of management accounting researchers.

There is another important cross-discipline area of ITG. Risk management has become much more important in ITG in recent years. A tangible example of this in the ITG domain is the

publication by ISACA of the RiskIT framework (ISACA 2009). The core elements of RiskIT have been incorporated in COBIT 5. RiskIT and COBIT 5 are explicitly designed to inter-operate with other frameworks, particularly the ISO 31000 risk management framework (ISO/IEC 2009). Wilkin and Chenhall (2010) point to several papers that relate to risk management in ITG. Many of these papers are only tangentially related to the nexus between ITG and risk management. There is much more to learn about this important element of ITG. Are there aspects of IT that make risk management in the IT arena different from other arenas? How do we understand, measure, simulate, and strategize IT risks? How does IT mitigate risk? How does IT create its own risk? Intuitively, the breadth and depth of the IT risk universe seem more challenging now than a decade ago. Is it? Understanding of risk management in the ITG domain involves a variety of disciplines, each with their own contribution. These include the traditional areas of finance and insurance, but also organizational behavior, psychology, and auditing. The risk management aspect of ITG seems ripe for a variety of research approaches, including building a better understanding of how enterprises are (or are not) successfully managing risk. Frameworks such as COSO, COSO-ERM, ISO 31000, and COBIT set out guidance on how entities should go about managing risk. Just how is this guidance reflected in the real world?

The papers in this theme issue employ a range of research methodologies including case study, survey, empirical archive, and field study. This diversity is likely to be an ongoing feature of ITG research. Given the relatively immature state of research on ITG, there will be a need for qualitative research. The study of Schobel and Denford (2013) in this issue is an example of a highly informative small sample size study. What are missing from ITG research at present are: in-depth case studies of ITG directions, successes, and failures.

—Roger S. Debreceeny
University of Hawaii at Manoa

REFERENCES

- Ali, S., P. Green, and A. Robb. 2013. Measuring top management's IT governance knowledge absorptive capacity. *Journal of Information Systems* 27 (1).
- Boritz, E. 2002. Information systems assurance. In *Research Accounting as an Information Systems Discipline*, edited by Arnold, V., and S. G. Sutton, 231–256. Sarasota, FL: American Accounting Association.
- Boritz, J. E. 2005. IS practitioners' views on core concepts of information integrity. *International Journal of Accounting Information Systems* 6 (4): 260–279.
- Boritz, J. E., and J. E. Hunton. 2002. Investigating the impact of auditor-provided systems reliability assurance on potential service recipients. *Journal of Information Systems* 16 (1): 69–87.
- Brynjolfsson, E., and A. Saunders. 2010. *Wired for Innovation: How Information Technology Is Reshaping the Economy*. Cambridge, MA: MIT Press.
- Chai, S., M. Kim, and H. R. Rao. 2011. Firms' information security investment decisions: Stock market evidence of investors' behavior. *Decision Support Systems* 50 (4): 651–661.
- Chen, R.-S., C.-M. Sun, M. M. Helms, and W.-J. Jih. 2008. Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese semiconductor company. *International Journal of Information Management* 28 (5): 366–378.
- Cragg, P., M. King, and H. Hussin. 2002. IT alignment and firm performance in small manufacturing firms. *The Journal of Strategic Information Systems* 11 (2): 109–132.
- De Haes, S., W. Van Grembergen, and R. Debreceeny. 2013. COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems* 27 (1).

- Debreceeny, R. S., and G. L. Gray. 2013. IT governance and process maturity: A multinational field study. *Journal of Information Systems* 27 (1).
- Fink, L., and S. Neumann. 2009. Exploring the perceived business value of the flexibility enabled by information technology infrastructure. *Information & Management* 46 (2): 90–99.
- Gordon, L. A., M. P. Loeb, and T. Sohail. 2010. Market value of voluntary disclosures concerning information security. *MIS Quarterly* 34 (3): 567–594.
- Héroux, S., and A. Fortin. 2013. The internal audit function in information technology governance: A holistic perspective. *Journal of Information Systems* 27 (1).
- ISACA. 2009. *The RiskIT Framework: RiskIT Based on COBIT*. Rolling Meadows, IL: ISACA.
- ISACA. 2011. *Global Status Report on the Governance of Enterprise IT (GEIT)—2011*. Rolling Meadows, IL: ISACA.
- ISACA. 2012. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). 2008. *ISO/IEC 38500: Corporate Governance of Information Technology*. Geneva, Switzerland: International Organization for Standardization/International Electrotechnical Commission.
- International Organization for Standardization/International Electrotechnical Commission (ISO/IEC). 2009. *ISO 31000: 2009 Risk Management—Principles and Guidelines*. Geneva, Switzerland: International Organization for Standardization/International Electrotechnical Commission.
- Janvrin, D. J., E. A. Payne, P. Byrnes, G. P. Schneider, and M. B. Curtis. 2012. The updated COSO Internal Control—Integrated Framework: Recommendations and opportunities for future research. *Journal of Information Systems* 26 (2): 189–213.
- Kwon, J., J. R. Ulmer, and T. Wang. 2013. The association between top management involvement and compensation and information security breaches. *Journal of Information Systems* 27 (1).
- Masli, A., V. J. Richardson, J. M. Sanchez, and R. E. Smith. 2011. The business value of IT: A synthesis and framework of archival research. *Journal of Information Systems* 25 (2): 81–116.
- Parent, M., and B. H. Reich. 2009. Governing information technology risk. *California Management Review* 51 (3): 134–152.
- Prasad, A., P. Green, and J. Heales. 2013. On governing collaborative information technology (IT): A relational perspective. *Journal of Information Systems* 27 (1).
- Ravishankar, M. N., S. L. Pan, and D. E. Leidner. 2011. Examining the strategic alignment and implementation success of a KMS: A subculture-based multilevel analysis. *Information Systems Research* 22 (1): 39–59.
- Schobel, K., and J. S. Denford. 2013. The chief information officer and chief financial officer dyad in the public sector: How an effective relationship impacts individual effectiveness and strategic alignment. *Journal of Information Systems* 27 (1).
- Tallon, P. P. 2007. A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems* 24 (3): 227–268.
- Tallon, P. P., and A. Pinsonneault. 2011. Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model. *MIS Quarterly* 35 (2): 463–484.
- Tambe, P., and L. M. Hitt. 2012. The productivity of information technology investments: New evidence from IT labor data. *Information Systems Research* 23 (3): 599–617.
- Velcu, O. 2010. Strategic alignment of ERP implementation stages: An empirical investigation. *Information & Management* 47 (3): 158–166.
- Wilkin, C. L., and R. H. Chenhall. 2010. A review of IT governance: A taxonomy to inform accounting information systems. *Journal of Information Systems* 24 (2): 107–146.
- Wright, S., and A. M. Wright. 2002. Information system assurance for enterprise resource planning systems: Unique risk considerations. *Journal of Information Systems* 16 (1): 99–113.