

Introduction

This position paper presents an overview of key insights on IT governance. The core concepts discussed in this paper are informed by ISO 38500, which is the internationally recognized standard that provides governing bodies and those who advise and assist them with guidance on how to effectively govern IT and meet compliance with their external regulatory obligations and internal policies. This standard, along with insights from pertinent academic and practitioner literature and subject matter experts, have informed the development of IVI's IT-CMF Governance (GOV) Critical Capability.

Relevance of IT Governance in the Digital Context

In the digital business environment, organizations have increased dependency on IT. Digital technologies, such as social, mobile, analytics, cloud and the Internet of Things, continue to transform the role of IT within organizations - from one of IT support to a strategy and technology partner [1]-[4]. In addition to providing a strong operational IT backbone, IT functions now need to be able to respond to new opportunities that are enabled by emerging technologies [5]. These technologies help organizations to expand internal dimensions, increase interaction with customers and external partners, improve IT services, integrate processes, disrupt markets, and fundamentally change entire industries [6]. Thus, IT-related investments are now recognized as core enablers of organizations' strategies [7, 8], supporting new business models and business practices [9]. However, organizations do not always realize intended benefits from such IT investments with high profile IT failures often resulting in organizational financial or reputational damage [10].

Many IT failures are a consequence of miscommunication between the governing bodies of organizations and their IT executives [11]. Thus, as IT becomes more pervasive in the organizational setting, there is now a need for an even greater focus on IT governance [12]. In a broad sense, this is concerned with directing and controlling the organization in order to achieve its goals [9]. It involves specifying decision rights and accountabilities for IT-related decisions to encourage desirable behaviour and guide appropriate and coherent decision-making regarding the use of IT in order to manage IT-related risks and maximize the potential benefits from IT investments. Being able to govern IT effectively is critical in today's organizations so that they are enabled to execute on their operational and strategic goals and to make and implement better decisions, faster [13]-[15]. Many research studies have found a correlation between effective IT governance and improved organizational performance [16]-[20]. For example, an MIT study of more than 250 organizations showed that those with above average IT governance performance when using a specific strategy were 20% more profitable than organizations with poor IT governance that followed the same strategy [18].

Despite the correlation between IT governance and organizational performance, in a recent MIT study, half of board members believed that their ability to oversee the strategic use of IT and digitally-enabled transformation projects was less than effective [21]. In fact, it is recognized that the maturity of the governance of key organizational assets varies considerably, with information assets being among those that are typically the worst governed [12]. This may be due to the complexities associated with governing IT effectively in the digital environment as it involves focusing attention on every facet of business models and business practices [9]. The changing demands placed on IT means that traditional IT governance models may not 'adequately reflect the realities of a digital world' [1].

Changing Nature of IT Governance in the Digital Context

Depending on the organization's context, the traditional top down chain of command/hierarchical model may no longer be appropriate in the digital context, as it inhibits employees further down the organization's hierarchy in making fast, informed decisions. Further, the view of IT being subjected to business authority no longer applies as IT becomes more business-aware and involved in high-level strategy development [1]. Structural arrangements for making IT-related decisions have become more complex, with decisions that were traditionally made by IT management now frequently made by non-IT executives often in geographically dispersed areas [14]. In fact, the locus of decision-making may rest at lower levels of the organization's hierarchy, making traditional top-down approval mechanisms obsolete [1].

Traditional approaches, whereby employees in different business units communicated via their senior representatives/managers, are becoming less effective. As processes become more enabled by digital technologies, multiple functional perspectives need to be integrated when developing new processes and applications [1]. IT and business representatives now need to work together more collaboratively [13]. Thus, joint decisions are now often made in cross-functional teams as opposed to traditional autonomous bilateral or functional level decision-making [1].

With the digitization of products and services the boundaries between IT and business processes are also blurred [1, 7]. As IT-enabled business processes are inseparable from IT, the traditional view of separated functional responsibilities may no longer be appropriate [1]. These changes have implications in terms of how organizations establish their IT governance arrangements, and how they evolve them to suit the digital shifts that are occurring.

Effective IT Governance in the Digital Context

The effective governance of IT in the digital context may necessitate new or improved governance structures, processes, and relational mechanisms [20], and a change in the organization's culture, shared beliefs, and behaviours regarding the use of IT. Thus, a prerequisite is to establish and sustain an enabling environment for IT governance. Central to such an enabling environment is the engagement of relevant internal stakeholders and the existence of clear leadership and commitment

from the organization's governing body and executive managers to set the organization's direction for the use of IT and to monitor its performance in achieving the required outcomes [10, 13, 22]. A sponsor and a small group or committee should be appointed by the governing body to oversee and drive the adoption or transformation of IT governance. In some organizations, this body is referred to as an IT governance steering group¹ [10, 22, 23]. Some organizations have also established innovation committees to identify opportunities from fast evolving digital technologies, and shared digital units to develop digital services for the rest of the organization [13]. The necessity of such committees or units is determined by the importance of IT in the organization's context and the organization's size [10].

IT governance should be guided by a set of principles that specify preferred behaviours, to guide decision-making in terms of the use of IT and how the organization establishes its IT governance mechanisms [8, 22]. These may include principles in relation to responsibility, strategy, acquisition, performance, conformance, and human behaviour [8]. Employee reward and incentive systems should be aligned with the behaviours these guiding principles aim to foster [18].

Authority and accountability for IT governance can be delegated to competent individuals (e.g. committees, sub committees, executive teams, business relationship managers) who will be answerable for IT-related decisions, actions, and performance [4, 8, 12]. These individuals should be enabled to act with autonomy and appropriate responsiveness in the changing business environment [22]. Delegated authority should be transparently recorded in a charter or in policy statements that outline the types of decisions that may be made by different individuals or structures (decision rights), who has input to those decisions (input rights), and the boundaries of those decisions. These may include decisions in relation to investments, IT architecture, IT sourcing, business strategy, as well as the governing body's reserve powers [10]. The appropriateness of the delegated authority should be regularly reviewed [8, 22]. In addition, the mechanisms through which individuals are held to account should be established and agreed (e.g. via performance and conformance evaluations) [14, 22]. Note: while authority may be delegated to the organization's management team for specific aspects of IT governance, accountability for the organization's overall performance and conformance and the effective, efficient, and acceptable use of IT remains with the organization's governing body [8, 22].

Rules, standards, and procedures for decision-making should be established outlining how decisions are to be reached and who is involved in the process [10, 14]. Such arrangements should be based on established strategies, policies, and decision-making responsibilities, authority, and boundaries [22], and should aim to support more simplified and accelerated decision-making. The decision-making arrangements should foster a more democratic culture whereby IT-aware business decision makers and business-aware IT decision makers are afforded a degree of autonomy in making decisions that

¹ The IT governance steering group (GSG) is responsible for ensuring transparent delegation of authority, tracking progress of change initiatives, and undertaking ongoing coordination and administrative activities related to IT governance, such as preparing the GSG's terms of reference, liaising with executive managers, collating the necessary information for monitoring and for the governing body to review [8].

are not within their immediate domains of expertise [1]. Reporting and exception handling arrangements should also be defined [22], to cater for 'maverick unsanctioned exceptions' that may occur with little organizational learning [18].

All relevant stakeholders should have a clear understanding of the purpose and objectives of IT governance [10]. Effective governance mechanisms need to reflect cross-functional learning and a unified understanding between IT and the business that results from overlap in their functional responsibilities. A growing emphasis on horizontal communication and increased transparency between, and integration across, organizational units are required [1]. Thus, communication approaches should be enhanced and education initiatives rolled out to encourage shared learning regarding the role of IT governance and future IT trends and directions [10, 12, 14, 22]. This is fostered through, for example, briefings on the governance framework and processes, the guiding principles, how business value can be derived through IT, how IT-related risks are managed [10, 22], and how IT governance is driven by corporate governance [24].

Having put the foundations in place to enable effective IT governance, the process of governing IT should focus on three core activities - evaluating, directing, and monitoring the current and future use of IT in the organizational setting [8]. The three activities should be carried out in close cooperation between the organization's governing body and its managers [22], so that the governing body can effectively guide or steer the organization's use of IT, rather than prescribe how it is done [10, 22].

The evaluate activities are concerned with making judgements regarding the current state use of IT, that is, how the organization is currently supported and enabled through the use of IT vis-a-vis the organization's business needs and objectives [8]. This involves evaluating current plans, proposals, supplier arrangements, and so on, and determining the extent to which desired outcomes are being realised (e.g. on a five-point evaluation scale of achievement). In undertaking this evaluation, there needs to be a clear understanding of factors in the organization's internal and external environments that may drive risks or opportunities and necessitate business change responses [8, 10]. Key factors in the internal environment include, for example, business goals and strategy, risk appetite, culture, change initiatives, key IT services, key IT-supported business processes, competence in the use of IT, and partner relationships. Key factors in the external environment include regulatory obligations, technological advances, generational trends, external threats, competitive forces, market developments, skills availability, and stakeholder requirements [10].

The direct activities involve defining the desired future state use of IT, that is, how the organization should be supported and enabled through the use of IT, and directing the development and implementation of strategies and policies², in accordance with the guiding principles, to achieve this desired state. In so doing, IT governance, as shaped by factors in the internal and external environment contexts, should align with that of the broader organization [8]. The desired state,

² There are two categories of policies: restraining policies that define the parameters within which decisions can be made (e.g. disaster recovery policies), and enabling policies which disseminate best practice (e.g. supplier relationship management policies) [14].

specifying the optimal outcomes for the organization, should then be defined (e.g. on a five-point evaluation scale) taking into consideration factors such as cost benefit analysis and readiness for change. Based on analysing the gap between current and desired states, an appropriate programme of change activities should be initiated to achieve the desired outcomes. This change programme needs to consider the required resources and skills, roles and responsibilities, inter-project dependencies, and quick-win deliverables, and reflect an appropriate prioritization of initiatives. The programme should be reviewed and approved by the governing board and have the requisite level of executive sponsorship for implementation [10].

The monitor activities are concerned with assessing the performance of IT and maintaining oversight of progress against plans, strategies, and objectives to guide further decision-making and to make informed adjustments. Evidence of success should be defined to measure the progress towards the achievement of outcomes and to determine the key areas of focus – such success measures may focus, for example, on benefits realization from IT investments, IT service delivery and service levels, risk and control, and information security. In addition, an appropriate measurement/monitoring system and (automated) reporting and audit practices should be established to compile and analyse data and present appropriate and timely reports to the governing body to track the change programmes and all evidence of success [4, 10]. Compliance with external and internal obligations (e.g. regulations, legislation, contractual agreements, internal policies, standards) should also be monitored [8].

The three core activities - evaluate, direct, and monitor - should be viewed in a continuous life cycle [12]. The organization should adopt a continual improvement approach to IT governance – setting an initial baseline and then focusing on opportunities for continual improvement of the governance arrangements to encourage desired behaviours [10, 13]. These will likely evolve over time in line with the rate of technology change, competitor initiatives, and the need to maintain alignment with changing organizational and environmental requirements [13, 14].

Conclusions

Ineffective IT governance in the digital context can result in missed opportunities and increases the risks associated with digital transformation [13]. However, being able to establish the appropriate IT governance for the organization results in a management paradox: it empowers employees across the organization in effectively using IT while simultaneously controlling compliance with the organization's vision, principles, and obligations [18]. Good IT governance will maximize the potential benefits from IT investments, by ensuring that appropriate and accelerated decisions are made regarding the current and future use of IT.

Evolution to an IT governance model that is appropriate in the digital context takes time. As digital transformation takes shape, governance systems will also be in a state of flux with old governance elements co-existing with new digital governance elements, at least temporarily [1]. Thus, finding the right approach for any organization is an incremental and experimental journey. Organizations that

want to understand and improve their IT governance capabilities have a structured and repeatable way to do so by using the IT-CMF Governance capability maturity assessment.

References

1. D. Arkhipova, G. Vaia, W. DeLone, and C. Braghin, 'IT governance in the digital era', *Working paper*, Department of Management, Ca' Foscari University of Venice, 2016. [Online] Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2847809.
2. J. Gottlieb and P. Willmott, 'The digital tipping point: McKinsey global survey results', McKinsey Quarterly, 2014. [Online] Available: <https://mobileservices.mckinsey.com/~media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/The%20digital%20tipping%20point%20McKinsey%20Global%20Survey%20results/The%20digital%20tipping%20point%20McKinsey%20Global%20Survey%20results.aspx>.
3. A. Main, B. Lamm, and D. McCormack, 'What boards need to know about digital transformation', *The Corporate Governance Advisor*, Jan/Feb, pp18-21, 2018.
4. PWC, 'Great by governance: improve IT performance and value while managing risks', 2014. [Online] Available: <https://www.pwc.com/us/en/industries/financial-services/library/viewpoints/information-technology-governance-improvement.html>.
5. H. Colella, T. Nunno, A. Rowsell-Jones, and M. Mesaglio, 'Three steps to successfully implementing bimodal-aware IT governance', 2012. [Online] Available: <https://www.gartner.com/doc/2901217/steps-successfully-implementing-bimodalaware-it>.
6. M. Spremić, 'Governing digital technology - how mature IT governance can help in digital transformation?' *International Journal of Economics and Management Systems*, vol.2, no.1, pp214, 2017.
7. A. Bharadwaj, O.A. El Sawy, P.A. Pavlou, and N. Venkatraman, 'Digital business strategy: toward a next generation of insights', *MIS Quarterly*, vol. 37, no. 2, pp471-482, 2013.
8. International Organization for Standardization (ISO), 'Information technology – governance of IT for the organization (ISO/IEC 38500: 2015)', 2015. [Online] Available: <https://www.iso.org/standard/62816.html>.
9. M. Toomey, *Waltzing with the elephant: a comprehensive guide to directing and controlling information technology*. Infonomics, 2009.
10. International Organization for Standardization (ISO), 'Information technology – governance of IT – implementation guide (ISO/IEC 38501: 2015)', 2015. [Online] Available: <https://www.iso.org/standard/45263.html>.
11. A.L. Holt, *Governance of IT – an executive guide to ISO/IEC 38500*. Swindon: BCS, 2015.

12. H. Hamidovic, 'Fundamentals of IT governance based on ISO/IEC 38500', *ISACA journal*, vol.5, 2010.
13. MIT-CDB and CapGemini Consulting, 'Governance: a central component of successful digital transformation', *Joint research programme on digital transformation*, 2012. [Online] Available: <https://www.capgemini.com/wp-content/uploads/2017/07/Governance_A_Central_Component_of_Successful_Digital_Transformation.pdf>.
14. J. Peppard, *IT governance workbook*. Information Systems Research Centre, Cranfield School of Management, nd.
15. J. Short, T. Nunno, and F. Caldwell, 'Gartner defines 'governance'', 2012. [Online] Available: <<https://www.gartner.com/doc/2145816/gartner-defines-governance>>.
16. A. Prasad, P. Green, and J. Heales, 'On IT governance structures and their effectiveness in collaborative organizational structures', *International Journal of Accounting Information Systems*, vol.13, no.3, pp199-220, 2012.
17. O. Turel, and C. Bart, 'Board-level IT governance and organizational performance'. *European Journal of Information Systems*, vol.23, no.2, pp223–239, 2014.
18. P. Weill, 'Don't just lead, govern: how top-performing firms govern IT', *MIS Quarterly Executive*, vol.3, no.1, pp1-17, 2004.
19. P. Weill, and J. Ross, *IT governance: how top performers manage IT decision rights for superior results*. Harvard Business School Press, Boston, 2004.
20. S.P.J. Wu, D.W. Straub, and T.P. Liang, 'How information technology governance mechanisms and strategic alignment influence organizational performance: insights from a matched survey of business and IT managers', *MIS Quarterly*, vol.39, no.2, pp497-518, 2015.
21. P. Weill and S. Woerner, 'Working with your board on digital disruption', MIT Sloan Management Centre for Information Systems Research, vol.XV, no.4, 2015.
22. International Organization for Standardization (ISO), 'Information technology – governance of IT – framework and model (ISO/IEC 38502: 2014)', 2014. [Online] Available: <<https://www.iso.org/standard/50962.html>>.
23. R. Huang, R.W. Zmud, and R.L. Price, 'Influencing the effectiveness of IT governance practices through steering committees and communication policies', *European Journal of Information Systems*, vol.19, no.3, pp.288-302, 2010.
24. J. Short, and M. Gerrard, 'IT governance must be driven by corporate governance', 2009. [Online] Available: <<https://www.gartner.com/doc/1229515/it-governance-driven-corporate-governance>>.

Contributing Authors

Dr Marian Carcary, Senior Lead Researcher, Innovation Value Institute.

Mr. Gerry Conway, Senior Research Fellow, Innovation Value Institute.

About IVI

The Innovation Value Institute (IVI) is a multi-disciplinary research and education establishment co-founded by Maynooth University and Intel Corporation. IVI researches and develops management frameworks to assist business and IT executives to deliver digitally enabled business innovation. IVI is supported by a global consortium of likeminded peers drawn from a community of public and private sector organizations, academia, analysts, professional associations, independent software vendors, and professional services organizations. Together, this consortium promotes an open ecosystem of research, education, advisory support, international networking, and communities-of-practice. IVI is supported through Enterprise Ireland's and IDA's Technology Centre programme.

Contact IVI

For more information on this capability, IT-CMF and other IT management topics, or on becoming a member of IVI's international research consortium, please visit www.ivi.ie or contact us at: ivi@nuim.ie or +353 (0)1 708 6931.



Innovation Value Institute, IVI, IT Capability Maturity Framework, and IT-CMF are trademarks of the Innovation Value Institute. Many of the designations used by manufacturers and sellers to distinguish their products are claimed as trademarks. Where those designations appear in this document, and the Institute was aware of a trademark claim, the designations have been printed with initial capital letters or all in capital letters.