A CORPORATE GOVERNANCE PERSPECTIVE ON IT GOVERNANCE

Anacleto Correia [*], Pedro B. Água [*]

* CINAV, Naval School, Military University Institute, Almada, Portugal

How to cite: Correia, A., & Água, P. B. (2021). A corporate governance perspective on IT governance. In S. Hundal, A. Kostyuk, & D. Govorun (Eds.), *Corporate governance: A search for emerging trends in the pandemic times* (pp. 107–114). https://doi.org/10.22495/cgsetpt19

Received: 28.04.2021
Accepted: 03.05.2021
Keywords: IT Governance, Corporate Governance, Control and Accountability, Risk Management, Enterprise Architecture
JEL Classification: M15
DOI: 10.22495/cgsetpt19

Abstract

IT governance encompasses the processes for aligning business and IT efforts to accomplish optimal value from the business by means of the implementation of effective IT control and accountability, performance and risk management. Despite IT governance awareness in recent years, there is a lack of a holistic view of the organization's IT governance that could help board directors to have an overall map of the current situation and anticipate the further steps needed to raise its level of maturity. This text proposes a classification scheme for IT governance according to two orthogonal dimensions: the stakeholders' perspective (from corporate board to end-users) as well as the primitives that are an object of IT governance. The proposed scheme, evolved from enterprise architecture research, is in line with other solutions aimed at aligning the business and IT within organisations.

1. INTRODUCTION

Information and communication technology (ICT) refers to the different types of communications networks and the technologies used for supporting business processes (OECD, 2021). Organizations' investment in ICT usually creates a complex and difficult to manage infrastructure, which includes disparate types of components, specifically: hardware (e.g., desktop computers, servers, mobile platforms and related peripherals); different operating system platforms; enterprise software platforms (pre-packaged, customised or in-house developed software) such as SCM, ERP, CRM, or KMS; networking and telecommunications

platforms; database management systems and other repositories; platforms based on internet technologies such as intranets and extranets web sites; and services such as consulting, outsourcing and systems integrators (Laudon & Laudon, 2020). In the near future, it is expected that the traditional ICT investment will increase driven by cloud, mobile, social and big data/analytics platforms. Furthermore, the emergence of new technologies will also contribute to significant spending in ICT, and, within the next decade, Internet of things (IoT), robotics, artificial intelligence, blockchain, and AR/VR will expand to represent over 25% of ICT investment (IDC, 2020).

The complexity in ICT architectures and infrastructures, and an increasing need for executives to ensure the value generation from organisation's business processes, will require an increasing awareness and understanding, by boards, of the role of IT Governance (Larsen, Pedersen, & Andersen, 2006). IT governance is a process aimed to align business and IT efforts to achieve an optimal value for the business through the joint and effective implementation of IT control and accountability, performance and risk management (Webb, Pollard, & Ridley, 2006).

The more the dependency of business on ICT the more concerns will be raised on how ICT is governed in order to ensure the performance, integrity, and continuity of businesses. Recent financial scandals (e.g., Enron, WorldCom, Lehman Brothers), unveiled the misuse of ICT to hide billions of dollars of bad debt, loans and inflation of earnings or assets through accounting loopholes. On the other hand, data breaches affecting well-known organizations (e.g., eBay, LinkedIn, Yahoo, Facebook) compromise organizations' security and privacy of billions of users whose stolen personal data (e.g., credit card numbers, email addresses, personal photos, passwords) were made publicly available or put up for sale on the dark web (Swinhoe, 2021). In such a kind of events — financial data's lack of integrity (Cheong & Chang, 2007), hardware or software failure, security breach or data leakage — compromising organisation's reputation and earnings, corporate boards are made legally accountable. Therefore, a holistic understanding of the IT governance role is crucial for effective corporate governance.

This text proposes a classification scheme, which provides a holistic view over IT governance, allowing the right actions to be triggered in order to correct business-IT misalignments and non-conformities on IT control and accountability, performance and risk management.

2. BACKGROUND

Management and governance are separate activities. Corporate governance is a responsibility delegated by shareholders and the public, defined by legislators and regulators, and shared by corporate boards, to some degree, with executive managers (Gill, 2002). Governance requires

a higher level of direction, leadership and control (Webb et al., 2006). Although the focus of corporate governance is more on the business than on technology, IT governance reflects a disposition to withdraw control and responsibility for IT from the CIOs and IT managers to be assumed by the board, where the ultimate accountability for business and technology alignment rests. IT governance, as a sub-set of corporate governance (Kingsford, Dunn, & Cooper, 2003), thus should be under the board sight (Webb et al., 2006). A convenient structure for decision-making should be implemented to facilitate the delegation of the responsibility to lower levels of the organisation both in IT and business departments. However, the board must always retain accountability and control.

Several definitions of IT governance are present in the literature (Webb et al., 2006). According to Korac-Kakabadse and Kakabadse (2001) IT governance is a process envisioning the following objectives: 1) assessment of the impact and nature of information systems, technology and communications; 2) development of the ICT skills bases; 3) increasing the relevance of business, legal and other ICT related matters; 4) protection of the interests of both internal and external stakeholders; and 5) raise the importance of the structure and quality of relationships among ICT stakeholders. For Van Grembergen, De Haes, and Guldentops (2004) IT governance has the following drivers: 1) strategic alignment; 2) delivery of business value through it; 3) performance management; 4) risk management; 5) control and accountability.

From the practitioners' point of view (ITGI, 2003) the purpose of IT governance is to direct IT processes, to ensure ICT performance meets the following objectives: 1) alignment IT and the business, realizing expected benefits; 2) enabling the organization to take advantage of opportunities and benefits through IT; 3) allow IT resources to be used correctly; and 4) mitigate IT risks. For the Information Technology Governance Institute (ITGI), IT governance needs three elements in order for the enterprise's IT to sustain and extend the enterprise's strategies and objectives: leadership, organizational structures, and processes. Additionally, ITGI highlights the shift of governance development from being driven primarily by the need for the transparency of enterprise risks and the protection of shareholder value, to the pervasive use of technology that created a critical dependency on IT, which calls for a specific focus on IT governance (ITGI, 2003).

Another perspective, highlighting the relevance of IT governance, is provided by the enterprise architecture (EA) perspective (Zachman, 1999; Sowa & Zachman, 1992). The purpose of enterprise architecture is to optimize processes across organizations, making it an integrated environment that is responsive for change while supportive of business strategy. Enterprise architecture addresses the need for effective

management and exploitation of information through IT, by providing a strategic context for the evolution of IT systems in response to the constantly changing needs of the business environment, achieving competitive advantage. Furthermore, a good EA enables the organization to achieve the right balance between IT efficiency and business innovation (TOGAF, 2018).

An EA framework, on the other hand, is a foundational structure, which can be used for developing a broad range of different interrelated architectures (e.g., business, information, information systems, technology). The framework usually contains a common vocabulary, a set of instruments, a list of recommended standards and a method for designing, departing from the current state of the organization, a target state defined by a set of building blocks (e.g., data, processes, applications, technologic infrastructure) that should fit together (TOGAF, 2018). Zachman (1999) in his seminal work about enterprise architecture, highlighted the building blocks of an EA.

Board directors can approach and support IT governance on an *ad hoc* basis and create its own framework, or can adopt a framework that has been developed and refined through the contribution and experience of several organizations and institutions. By adopting an IT governance holistic perspective, boards can have a framework for grouping methods, tools, applications, and standards in one classification scheme. The presented proposal intends to systematize the main concepts of IT governance represented within the same framework.

3. PROPOSAL

Within the scope of this text, and using the concept of symmetry, the classification scheme proposed by Zachman (1999) is applied to IT governance. The rationale for this analogy is grounded in the realization that IT governance addresses the same building blocks of the enterprise architecture. Therefore, for sake of symmetry, it is suggested the parity of the IT governance elements with the building blocks of the enterprise architecture.

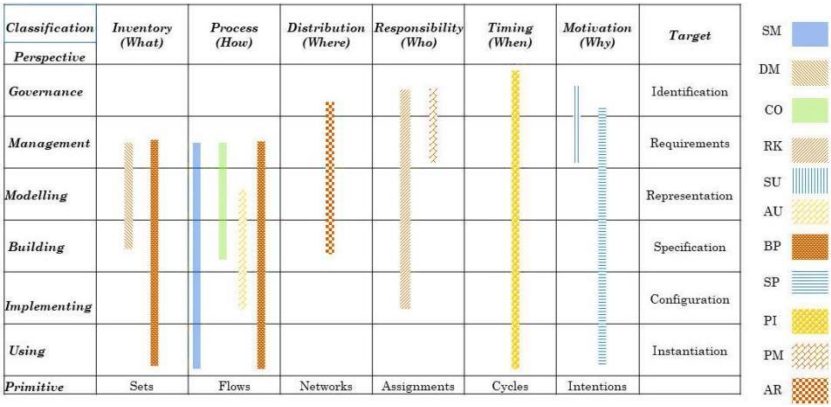
The concept of symmetry in architecture is ancient. According to Roman architect Vitruvius, symmetry consists of the union and conformity of the parts of a work, in relation to its totality. Symmetry also derives from the Greek concept of analogy, which is understood as the relationship between all parts of a structure with the whole structure. That is why a uniform symmetry between IT governance and enterprise architecture is required. In general, uniform symmetry occurs in architecture when the same motif reigns throughout the structure.

The proposed classification scheme for IT governance (Table 1) is depicted as a two-dimensional matrix composed by: 1) rows as top-down *perspectives* on IT governance, from contextual corporate board perspective to end-users' operations perspective, and 2) columns as

primitive concepts, triggered by interrogative adverbs. Each perspective in the first dimension aims at a *target* (i.e., the reification of abstract ideas into instantiation), labelled as *Identification*, *Requirements*, *Representation*, *Specification*, *Configuration*, and *Instantiation*. Each one of the reification levels corresponds to a different organizational level with different perspectives of their role in what IT resources concerns: *Governance*, *Management*, *Modelling*, *Building*, *Implementing*, and *Using* (corresponding to the board, executive directors, data and process modellers, IT supervisors, IT implementers, and IT stakeholders — such as internal or external users, auditors, IT suppliers, regulators, clients). The second dimension intends at the elicitation of a certain type of artifacts built in response to specific adverbs: *Inventory* (What), *Process* (How), *Distribution* (Where), *Responsibility* (Who), *Timing* (When), and *Motivation* (Why). Each column elicits artifacts derived from the following primitive concept: Sets, Flows, Networks, Assignments, Cycles, and Intentions. The final classifications are depicted as cells resulting from the intersection between the perspectives and the concepts and filled by the methods, tools, applications, and standards used in IT governance. The overall matrix constitutes the total set of instruments that are relevant for dealing with any architectural part of an organization, through IT governance, as well as the overall organization itself.

A variety of IT governance instruments currently available were used to fill the matrix in Table 1, bearing in mind the rationale for the orthogonal axes. Some of these instruments were developed as a set of guidelines, others as methods, tools, applications, best practices, and still others as *de facto* or *de jure* standards. In the next paragraphs, a list of instruments that were added to the classification scheme is presented.

Table 1. Classification scheme for data governance



1. *SM: Instruments for management of IT services:*
- Information Technology Infrastructure Library (ITIL4);
- ISO/IEC 20000:20118 is international standard for service management;
- Application Services Library (ASL2) is a framework to standardize processes within application management;
- Business Information Services Library (BiSL) is a framework that describes processes within business information management at a strategic, management and operational level.

2. *DM: Instruments for data management:*
- ISO/IEC 11179 is a standard for representing metadata for an organization;
- ISO/IEC 21838 is a standard for top-level ontologies;
- ISO 15926 is a standard for data integration, sharing, exchange, and hand-over between computer systems.

3. *CO: Instruments for linking and measuring business and IT goals:*
- COBIT (control objectives for information and related technologies);
- ISO/TC 309 is a standard for the governance of organizations;
- ISO/IEC 38500 is a standard for corporate governance of information technology.

4. *RK: Instruments for risk management:*
- ISO 31000 — family of standards related to risk management;
- Committee of Sponsoring Organizations of the Treadway Commission (COSO);
- Sarbanes-Oxley Act (SOX) set requirements for US public company boards, management and public accounting firms;
- Basel II-IV is a set of recommendations on banking laws and regulations;
- ISO 37001 is a standard that sets out the requirements for an anti-bribery management system (ABMS).

5. *SU: Instruments for address sustainability requirements:*
- ISO 14000 is a family of standards related to environmental management;
- ISO 26000 is an international standard providing guidelines for social responsibility.

6. *AU: Instruments for auditing:*
- Statement on Standards for Attestation Engagements No. 18 (SSAE 18) is a generally accepted auditing standard focused on reporting on the quality of financial reporting;
- ISAE 3000 is the standard for assurance over non-financial information;
- ISAE 3402 provides assurance to an organization's customer that the service organization has adequate internal controls.

7. *BP: Instruments for management of business and knowledge processes:*
- Business intelligence (BI);
- Business process management system (BPMS);
- Enterprise resource planning (ERP) systems;
- Supply chain management (SCM) systems;
- Customer relationship management (CRM) systems;
- Knowledge management systems (KMS).

8. *SP: Instruments for the management security and privacy:*
- ISO/IEC 27000 is a family of standards for information security management systems (ISMS);
- the General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy;
- ISO 28000 is a family for security management systems for the supply chain.

9. *PI: Instruments for process maturity improvement and assessment:*
- Capability Maturity Model Integration (CMMI).

10. *PM: Instruments for project management:*
- Project Management Body of Knowledge (PMBOK);
- ISO 21500 is an international standard providing good practice in project management;
- ISO 10006 is an international standard providing guidelines for quality management in projects.

11. *AR: Instruments for systems architecture:*
- ISO/IEC/IEEE 42010 is an international standard for architecture description of systems and software engineering;
- TOGAF is a framework for enterprise architecture.

4. CONCLUSION

Nowadays organizations use IT as the main infrastructure for directing business. For an adequate business-IT alignment this relationship should be adequately governed at all institutional levels (perspectives), for all primitive resources used. In this paper, we propose a classification scheme for IT governance. The tool, derived from an enterprise architecture framework, intends to be a map for corporate boards in the pursuit of IT governance. As future work, the proposed model will be developed by exploring and deepening the relationships raised between IT governance and enterprise architecture.

REFERENCES

1. Cheong, L. K., & Chang, V. (2007). The need for data governance: A case study. In *ACIS 2007 Proceedings — 18th Australasian Conference on Information Systems*. Retrieved from https://core.ac.uk/download/pdf/301346974.pdf

2. Gill, M. (2002). Corporate governance after Enron and World.com. Paper presented at the *Insight Conference on Corporate Governance*. Retrieved from https://bit.ly/2S2su1b
3. IDC. (2020). *Global ICT spending: Forecast 2020–2023*. Retrieved from https://bit.ly/32NpU0U
4. ITGI. (2003). *Board briefing on IT governance* (2nd ed.). IT Governance Institute. Retrieved from https://bit.ly/3uG09eh
5. Kingsford, R., Dunn, L., & Cooper, J. (2003). Information systems, IT governance and organisational culture. Paper presented at the *14th Australasian Conference on Information Systems*.
6. Korac-Kakabadse, N., & Kakabadse, A. (2001). IS/IT governance: Need for an integrated model. *Corporate Governance, 1*(4), 9–11. https://doi.org/10.1108/EUM0000000005974
7. Larsen, M. H., Pedersen, M. K., & Andersen, K. V. (2006). IT governance: Reviewing 17 IT governance tools and analysing the case of Novozymes A/S. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2006.234
8. Laudon, K. C., & Laudon, J. P. (2020). *Management information systems: Managing the digital firm* (Global 16th ed.). Upper Saddle River, NJ: Pearson Education, Inc.
9. OECD. (2021). *ICT investment (indicator)*. https://doi.org/10.1787/b23ec1da-en
10. Sowa, J. F., & Zachman, J. A. (1992). Extending and formalizing the framework for information systems architecture. *IBM Systems Journal*, *31*(3), 590–616. Retrieved from http://www.jfsowa.com/pubs/sowazach.pdf
11. Swinhoe, D. (2021, January 8). The 15 biggest data breaches of the 21st century. *CSO*. Retrieved from https://bit.ly/3g7D68M
12. TOGAF. (2018). *Welcome to the TOGAF® Standard, Version 9.2, a standard of The Open Group*. Retrieved from the Open Group website: https://pubs.opengroup.org/architecture/togaf9-doc/arch/
13. Van Grembergen, W., De Haes, S., & Guldentops, E. (2004). Structures, processes and relational mechanisms for IT governance. In W. Van Grembergen (Ed.), *Strategies for information technology governance* (pp. 1–36). https://doi.org/10.4018/978-1-59140-140-7.ch001
14. Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences*. https://doi.org/10.1109/HICSS.2006.68
15. Zachman, J. A. (1999). A framework for information systems architecture. *IBM Systems Journal*, *38*(2.3), 454–470. https://doi.org/10.1147/sj.382.0454