Gaps Between Theory and Practice on IT Governance Capabilities

Oscar González-Rojas, Juan E. Gómez-Morantes and Guillermo Beltrán

Abstract Nowadays, Information Technology (IT) governance is a core activity either adopted or at least expected by most organizations, to control the behavior of IT assets. However, this discipline faces a growing gap between the views, priorities and practices of academics and practitioners. This paper presents a consolidated view of capabilities for implementing IT governance within an organization. We evaluated such capabilities in the practice of Colombian companies within the logistics industry. The main gaps that arise when adopting IT governance capabilities are discussed, and research insights are provided for aligning theory and practice.

Keywords IT management · ICT governance · Capability model
Business-ICT alignment · Risk management

1 Introduction

Initially considered as a sub-set of corporate governance, IT Governance (ITG) has emerged as its own discipline since the 90s [1]. Even though the term ITG did not gain traction in literature until the late 90s, similar concepts were used as early as 1963 [2]. Later, in the mid-2000s, evidence about the link between ITG and

A prior version of this paper has been published in the ISD2017 Proceedings (http://aisel.aisnet.org/isd2014/proceedings2017).

O. González-Rojas (✉) · G. Beltrán
Systems and Computing Engineering Department, Universidad de los Andes,
Bogotá, Colombia
e-mail: o-gonza1@uniandes.edu.co

G. Beltrán
e-mail: ga.beltran66@uniandes.edu.co

J. E. Gómez-Morantes
Systems Engineering Department, Pontificia Universidad Javeriana, Bogotá, Colombia
e-mail: je.gomezm@javeriana.edu.co

N. Paspallis et al. (eds.), *Advances in Information Systems Development*,
Lecture Notes in Information Systems and Organisation 26,
https://doi.org/10.1007/978-3-319-74817-7_9

performance in large organizations [3] generated great interest from both academics and practitioners. Since then, an ample body of literature has been published regarding different aspects of ITG.[1] However, most of this literature is focused on the definition of ITG and its dimensions, the benefits of proper ITG schemes, contingency research looking for the most appropriate ITG model in a given scenario [4], and prescriptive models of ITG implementations [5, 6].

While this stream of research has achieved important milestones in the field, it is becoming evident that there is a growing gap between the views, priorities and practices of academics and industry practitioners (see Sect. 2.2). In order to understand the roots and impacts of this gap, it is important to increase the empirical base of ITG research as a way to build stronger bridges between these communities and to allow for ITG research to be better informed by actual ITG practice; something essential to close the theory-practice gap discussed in this paper.

The remainder of this paper is as follows. In Sect. 2, we discuss current issues on ITG research by emphasizing on related work on ITG gaps between research and practice. Section 3 discusses the methodological approach we followed to identify the gap between the ITG practices proposed in the literature and those used by practitioners. Section 4 describes a capabilities model created to consolidate ITG literature. Section 5 presents the ITG practices of four Colombian companies of the logistics sector and compares them with the capabilities model. As a result, we present the identified gaps and a characterization of the capabilities of this industry. Finally, conclusions and future work are presented in Sect. 6.

2 IT Governance: Context, Issues, and Gaps

Multiple definitions of ITG have been proposed from different perspectives and with different focuses and objectives [1, 7]. From a more practice-focused perspective, plenty of literature exists covering ITG frameworks, implementation processes, and good practices. This is a difficult issue because the lack of consensus within the academic community about the very definition of the concept hinders any advancement in the field. Furthermore, the lack of consensus between academics and practitioners about this definition affects the communication between these groups, and reduces the chances of collaboration between them [8].

The issue of multiple ITG definitions has been debated in recent literature [1, 2]. It is now commonly accepted that the core of ITG is composed by four dimensions: (a) the allocation of IT decision making rights, (b) the management of IT risks, (c) the mechanism to align IT decisions and business strategy, and (d) organizational structures to monitor and control IT decisions. As suggested by Weill, "IT Governance is not about what specific decisions are made, that is management" [3].

[1] More than 30,000 publications found in Google Scholar using the query "IT Governance".

This means that ITG is about the specification and implementation of organizational structures and processes that are in charge of making and monitoring IT decisions.

2.1 Current Issues on IT Governance Research

Parting from the definition of ITG presented earlier, it is now time to examine some of the limitations of the concept and current research issues in the field. One of the main gaps in ITG research is its dynamic nature. New literature is required to analyze the conditions that will result in a change in ITG over time, as well as the transition process from one model to another. This issue is relevant not only because the current business climate is one of constant change and disruption, but also because advancements in the IT field (e.g. cloud computing) are challenging our current knowledge about ITG and how it is performed [9].

Another issue regarding ITG research is the limitations of the rational theories used so far to study this phenomenon. According to Jacobson, ITG scholars have relied too much on what he calls rational theories of the organization; theories that "are based in economics and assume managers' ability to systematically be aware of, rank, and then choose best alternatives based on certain criteria (e.g. costs and benefits) to achieve a desired outcome (e.g. improved efficiency)" [5]. The biggest issue with the over-reliance on these rational theories is that they are not well equipped to understand some of the social aspects of ITG such as change, improvisation, external influences, politics, etc. Finally, there is the issue of gaps between theory and practice in ITG. Since this issue is the focus of this paper, it is discussed in more detail below.

2.2 Gaps Between Theory and Practice

Since IT issues include multiple actors (e.g. IT producers, consultants, client organizations, regulators, users, academics, etc.), it is easy to find disconnections between them. In ITG literature, the theory-practice gaps are one of the most relevant gaps. These particular kinds of gaps can be defined as a disconnection between practitioners and the main body of literature in the discipline (i.e. academic publications, standards, frameworks). It is important to note, however, that a disconnection between theory and practice should not be confused with a lack of knowledge from practitioners, as practitioners, despite being fairly familiar with the literature, can choose to depart from it. This distinction is important because the objective of researching theory-practice gaps is to highlight the areas in which practitioners can inform the literature and open new research avenues.

These gaps between ITG definitions and representations have been discussed by multiple authors. Keyes-Pearce [8] compares practitioners' motivations in the implementation of IT models or processes in their organizations, against the managerial drivers expressed in academic publications on ITG. The author found that the motivations for the adoption of ITG models diverge from the "IT as a source of competitive advantage" discourse encountered in the literature and are closer to a more pragmatic "IT as a competitive necessity" discourse. Additionally, the author noticed that practitioners are often unable to articulate what ITG means for them. Ko and Fink [10] studied gaps in three dimensions of ITG: structures, people, and processes. Even though they do not provide any explicit definition of gap, a reader could infer that they understand gaps as any ITG decision that deviates from the literature. This approach, however, can be criticized for being slightly pro-literature because it assumes that the positions of the ITG literature are superior to those of practitioners, without much discussion.

Simonsson and Ekstedt [7] studied the ways in which industry and literature assigned priorities to different components of the ITG definition. Using a survey-based methodology, the authors concluded that even though there are no major differences in the priorities of these groups, there are some differences in the priorities assigned by them. Regarding the decision making process, practitioners tend to give more priority to the understanding phase of the process, while the literature gives more importance to the monitoring phase of the process. Also, practitioners assign less importance to tactical issues than the literature. Willson and Pollar [6] present an in-depth study of ITG practices in a large Australian organization. In this case, the authors found practices not currently covered in the ITG literature like performance measuring as a tool in ITG. Furthermore, the authors found factors like organizational history and nature that have a significant impact on ITG models and practices. This case is instrumental in arguing that the academic literature can learn a lot from studying actual ITG practices. Finally, Winkler et al. [11] focused on the structural elements of ITG to explore the impacts of new technology models, like the Software as a Service (SaaS), on current ITG practices.

In summary, the current literature on ITG theory-practice gaps can be classified into three categories: ontological gaps, ITG antecedents' gaps, and dynamic gaps. Ontological gaps refer to the differences concerning what an ITG is, how it is performed, and which factors are important in its practice. Antecedents gaps refer to the importance of ITG, the business imperative of ITG efforts, and the priorities on ITG practices vs those expressed by the literature. Finally, dynamic gaps refer to the lack of literature on the change and evolution of governance practices.

3 Research Methodology

In order to contribute to a better understanding of theory-practice gaps in ITG, the main research question (RQ) of this paper is as follows: What are the differences between the ITG practices proposed in the literature and those actually used in practice?

Because of the complexity of ITG practices and the importance of gathering detailed information to measure theory-practice gaps in ITG, this paper adopts a qualitative approach based on the case study method. The case studies follow a multiple-case design with embedded units of analysis [12] to introduce an element of triangulation at the empirical level, thus improving the veracity of the findings.

The main four companies within the logistics and transportation industry in Colombia were selected as case studies. Two of them have presence exclusively in Colombia while the other two are multinational companies; we only analyzed the Colombian subsidiary of the latter. The companies' sizes range from 800 to 3000 employees. Between one and three in-depth interviews with high ranking managers (e.g. CIO, CEO) were performed for each case. The interviews followed a semi-structured model based on a survey of 49 questions. The questionnaire was designed around four embedded units of analysis (i.e. the four ITG dimensions that were identified in Sect. 2) by covering ITG concerns such as vision, current practices, undesired IT behaviors, decision-making archetypes among business units, strategic and operational mechanisms, among others.

The data analysis is based on an ITG capabilities model (see Sect. 4) that represents expected ITG actions (what to do) and specific ITG capabilities to perform those actions (how to do it) based on different frameworks and academic literature. This model decomposes actions and capabilities within three levels: strategic, tactical, and operational. This decomposition aims to highlight important areas for the evaluation and research of existing ITG theory-practice gaps. The data gathered in the interviews was used to build an ITG practices profile for each company. These profiles were then compared to the capabilities model and a gap analysis was performed. This allows for the measurement of the gap between theory (represented in the capabilities model) and practice (represented in the profiles).

This research has two main limitations. On the one hand, it only includes Colombian companies from the logistics industry and, since ITG issues are highly contingent (i.e. they depend on the context), the data and conclusions presented in this research could differ from those obtained in other regions or industries. The second limitation is related to the methodology used in this research. Since only four cases were selected, this research does not present any statistically significant results that could be generalized to other populations. However, it is important to note that this research does not intend to achieve generalizability to populations but to theoretical elements. This means that the value of this research does not lie in any predictive or prescriptive statement, but in the ITG capability model presented in Sect. 4 as a tool to evaluate ITG theory-practice gaps.

4 Core Capabilities on IT Governance

A Capability is a particular ability that an organization or system has in order to achieve a specific goal [13]. These abilities are enabled by a combination of resources (e.g. people, processes, IT) and by how those resources are managed [14].

Therefore, the application of ITG capabilities and their continuous improvement and evolution over time can differentiate the companies within an industry.

We created a capabilities model by aggregating different sources of information regarding ITG. These capabilities were grouped into four dimensions (decision-making, risk management [15], value delivery and alignment, and performance management [15]) and then characterized into three levels (strategic, tactical and operational capabilities).

Strategic capabilities refer to high-level decision-making grants and guidelines defined to control IT assets. Tactical capabilities refer to the coordination of activities and resources to enforce a given decision or guideline. Finally, operational capabilities refer to concrete day to day actions to automate and control ITG activities. These capabilities do not pretend to guide how ITG must be performed; they are a summary of the expected actions presented in the literature. Thus, multiple and contrasting capabilities can be performed to achieve a desired ITG state.

Table 1 summarizes the core actions and capabilities identified regarding decision-making rights and responsibilities on ITG [3].

Table 2 describes the actions and capabilities identified for the value delivery and alignment dimension. This dimension focuses on using IT investments as linkages between company-wide ITG, business unit levels and the project team level, both for the business and IT. Such linkages represent value to the organization as a whole [20].

Table 3 describes the core actions and capabilities identified in regards to risk management on ITG. Risk management covers the unplanned events that may represent an IT failure, which could threaten enterprise goals due to IT pervasiveness [17].

Table 1 Actions and capabilities to support the decision-making dimension

	Action (What)	Capabilities (How)
Strategic	1. Establish desired IT behavior [3] 2. Establish decision accountability on IT Principles, Enterprise Architecture, Business Application Needs, IT Infrastructure, IT Investment and prioritization [3] 3. Establish input rights on decisions [3] 4. Identify archetypes per decision type (e.g. Monarchy, Federal, IT Duopoly, Feudal) [3]	**Structures** 1. Committees (Executive Committee, IT Leaders Committee, Process Team, Account Managers) [3] **Information/Artefacts/Resources** 2. Decision maps per delegation of authority (accountabilities) and archetype [3] 3. Politics for exception handling [3] 4. Internal communication mechanisms (e.g. web portals) [3]

(continued)

Table 1 (continued)

	Action (What)	Capabilities (How)
Tactical	1. Evaluate conflicts on decision-making 2. Evaluate impact on decision-making (risks, profit, asset utilization, growth) 3. Coordinate decision-making according to the desired IT behavior 4. Prioritize the IT processes to be designed and implemented (an implementation roadmap) [16]	**Processes** 1. Coaching stakeholders that are not following decision rules [3] **Information/Artefacts/Resources** 2. Agreement definition (SLA, OLA, UC) [3] 3. Definition of target decision maps [16] 4. Coaching stakeholders not following decision rules [3] **Communication** 5. Managerial alerts [3]
Operational	1. Define control on decision making [3] 2. Specialize generic decisions within the five strategic decision categories	**Processes** 1. Audit procedures [17] 2. Measuring asset utilization—COBIT EDM04 ensure resource optimization [18] 3. Monitoring of agreements—COBIT APO09 manage service agreements [18] 4. Processes on IT frameworks (e.g. COBIT [18], ITIL [19]) **Information/Artefacts/Resources** 5. IT Metrics regarding decision rights [3]

Table 2 Actions and capabilities to support the value delivery and alignment dimension

	Action (What)	Capabilities (How)
Strategic	1. Establish guidelines for value delivery measurement [18] 2. Prioritize investment initiatives based on clearly defined criteria (e.g. higher benefits, less risk) [3, 18]	**Structures** 1. Board of directors [18] 2. Management Committee [18] 3. Project Management Office (PMO) [18] 4. IT executives with deep understanding of business environment [21] **Processes** 5. Project management [18]
Tactical	1. Manage IT value generation and delivery [18] 2. Identify opportunities for IT portfolio improvement [18] 3. Prioritize new IT investments and projects [18]	**Structures** 1. Project Management Office (PMO) [18] **Processes** 2. Definition of metrics with non-financial value [18]

(continued)

Table 2 (continued)

	Action (What)	Capabilities (How)
	4. Evaluate IT portfolio distribution after organizational changes [18]	3. Quantification of non-financial metrics [22] 4. Processes of IT investment portfolio management—COBIT process BAI01 Manage Programmes and projects [18] **Information/Artefacts/Resources** 5. Financial value metrics (e.g. ROA, ROI, ROE, NPV) [3] 6. Ratio between IT operation costs and obtained benefits [18]
Operational	1. Evaluate benefits generated by IT services, assets and investments defined on the IT portfolio [18] 2. Implement new IT investments and projects following a project management methodology [18] 3. Quantify the business value delivery from IT services 4. Measure the value generated between architectures 5. Calculate the value flow between architectures 6. Project the value of IT services	**Processes** 1. Calculation of benefits generated by IT services and investments defined on the IT portfolio [18] 2. Calculation of the financial value delivered to the business, regarding IT services behavior (risks, service agreements, costs, income, and alignment) [28] **Information/Artefacts/Resources** 3. Metrics by asset [18] 4. Project management methodology [18] 5. Value flow measurement techniques

Table 3 Actions and capabilities to support the risk management dimension

	Action (What)	Capabilities (How)
Strategic	1. Plan and direct risk management [23] 2. Align IT risk policy with corporate risk policy [18] 3. Build a risk-aware culture [17] 4. Define and implement a risk governance process [17]	**Structures** 1. Executive level (Board of directors, management committee) [17, 18] **Information/Artefacts/Resources** 2. Risks map 3. Risk appetite and tolerance [18] **Processes** 4. COBIT Process EDM03—Ensure Risk Optimization [18] 5. List of breaches that executives could be accountable for [24]

(continued)

Table 3 (continued)

	Action (What)	Capabilities (How)
		6. Segmented audiences based on their role towards risk awareness [17]
Tactical	1. Assess IT-related risks that may affect the organization [18] 2. Create and maintain an IT risk management portfolio [25] 3. Align IT risk management with corporate risk management	**Structures** 1. Management committee [3] 2. IT specialized committees [3] **Processes** 3. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) processes for assessing risks on Information Security [26] 4. Risk policies and standards [23] 5. COBIT process APO12—manage risks (create and maintain a formal document with the identified risks) [18] **Communication** 6. COBIT process EDM03.02 (channels to deliver the campaigns to all the employees) [18]
Operational	1. Collect and analyze information regarding IT risks [17] 2. Perform a cost-benefit analysis on risks [17] 3. Design and prove a business continuity plan [17] 4. Identify and close vulnerabilities in the IT assets base [17] 5. Implement controls and industry best practices [18] 6. Simulate solution scenarios to control risks 7. Report risks materialization [18]	**Structures** 1. Service manager [18] 2. Business-IT Council [3] 3. IT specialized committees [3] 4. IT Audit [3, 17, 27] **Processes** 5. COBIT process APO12.01—Manage Risks [18] 6. Risk quantification of operational assets (processes, IT services) [28, 29] 7. Business Impact Analysis (BIA) [17] 8. Business continuity plan with responsible and expected quality of service levels [17] 9. IT audits [27] 10. COBIT process APO12.02 (Cost-benefit analysis on risks treatment) [18] **Information/Artefacts/Resources** 10. List of critical IT assets and their vulnerabilities [26] 11. Test environments [18] **Communication** 12. Channels to notify materialization of a risk to whomever is responsible

Table 4 describes the actions and capabilities identified for the performance management dimension. This dimension covers the definition, monitoring and evaluation of business and IT goals and metrics against expected performance goals [18].

Table 4 Actions and capabilities to support the performance management dimension

	Action (What)	Capabilities (How)
Strategic	1. Identify agreements with the stakeholders regarding the expected performance of IT investments [18] 2. Manage the use of IT resources	**Structures** 1. Executive committee [3, 18] 2. IT specialized committees [3] **Processes** 3. Models of IT agreements or contracts [18] 4. Measurement of resources use (time, costs) [18]
Tactical	1. Specify agreements with the stakeholders regarding the performance goals and metrics expected from IT [18] 2. Rationalize asset use 3. Evaluate IT performance on profit, asset utilization, growth [3]	**Structures** 1. Management committee [3] **Processes** 2. IT performance on profit (executive committee, architecture process, capital approval, tracking of business value) 3. IT performance on asset utilization (Business/IT relationship manager, Process teams with IT members, SLA and Chargeback, IT leadership decision making body) 4. IT performance on growth (budget approval, risk management, local accountability, portals)
Operational	1. Monitor performance of IT services, assets and investments so as to identify improvement opportunities 2. Manage IT assets [18] 3. Manage utilization of human resources among multiple business processes 4. Collect information on the performance of the IT services and assets defined in the IT portfolio [18]	**Processes** 1. COBIT process MEA01-Monitor and evaluate performance and conformance [18] 2. COBIT process BAI09-Manage Assets [18] 3. COBIT process APO07-Manage human resources [18] **Information/Artefacts/Resources** 4. Map of IT assets and corporate processes supported by those assets [18] 5. IT portfolio [18]

5 Measuring Gaps on IT Governance Capabilities

5.1 Assessment Criteria

Table 5 describes how the capabilities defined in Sect. 4 can be evaluated in terms of two elements: existence and function. This means that an organization has capabilities not just because it has an ITG structure but because this structure performs certain tasks as well.

Table 5 Expected evidence on IT governance capabilities

	Strategic	Tactical	Operational
Decision-making support	DS1. Decisions are explicit DS2. Decision-making structures are defined DS3. Decisions made among different structures are aligned DS4. Decision-making responsibilities are clearly defined DS5. The decision-making archetype is known and aligned with expected IT behavior	DT1. Decision-making archetypes are defined and recognized for each type of decision DT2. The agreements on decisions are formally defined DT3. Framework implementation initiatives consider stakeholders to create an implementation plan DT4. Decisions are made only by those formally defined to make them	DO1. All decisions are clearly identified and classified into one of five decision types DO2. Governance model is based on proactive mechanisms over reactive ones DO3. Defined agreements are periodically monitored using technical tools
Risk management	RS1. There is an organizational risk awareness culture RS2. Risk appetite and tolerance are formally defined RS3. There is a formally defined IT risk policy, aligned with the corporate risk policy RS4. Risk awareness programs are implemented within the organization	RT1. IT risks that may affect the organization are clearly identified and assessed RT2. There is a formal definition of owners and managers that are responsible for IT risk RT3. There is an IT risk management portfolio that collects information on the identified risks	RO1. Cost-benefit analyses of IT risks are performed periodically RO2. A business continuity plan is defined and tested periodically RO3. Controls over IT risks are implemented based on cost-benefit analysis and industry best practices RO4. IT risks are quantified RO5. IT audits are performed regularly to identify and close vulnerabilities over IT assets
Value delivery and alignment	VS1. There are clearly defined guidelines to measure value delivery VS2. IT investments are prioritized based on specific criteria (e.g. higher benefits, lesser risk)	VT1. IT portfolio is constantly monitored to assure the transfer of benefits VT2. Organization is constantly looking for investment opportunities to improve the IT portfolio	VO1. There is an IT portfolio that contains information on IT services, assets and investments VO2. IT investment and projects follow project management methodologies VO3. The business value delivery from IT services is quantified

(continued)

Table 5 (continued)

	Strategic	Tactical	Operational
		VT3. New IT investment initiatives are prioritized according to organizational criteria VT4. IT portfolio is periodically reviewed to keep it updated with organizational changes	
Performance Management	PS1. There is a formal definition of expected performance of IT services, from the stakeholders PS2. There is an understanding of the business value delivered by IT	PT1. Formal agreements of expected performance are defined with stakeholders PT2. Formal evaluations are executed to measure IT performance	PO1. IT services are evaluated against stakeholders' expectations PO2. IT assets are periodically evaluated to guarantee that they are used effectively to support business requirements PO3. Human resources are used effectively to support multiple business processes

5.2 Gap Analysis for the Logistics Industry

Based on the previous criteria, this section presents the most significant theory-practice gaps that we identified after evaluating the ITG capabilities of the four companies mentioned in Sect. 3. After performing this analysis, we identified an approach that can be taken as a characterization of the sector.

Since decision-making is important for most companies at the strategic level, the three analyzed companies had clearly defined decision-making structures and critical decisions to control. However, there was a lack of mechanisms (e.g. decision maps) to align decisions made from different structures. At the tactical level, only one company had formally defined service level agreements and controlled decisions, which could only be made by the defined structures. The lack of agreements in the remaining three companies generated conflicting decisions. All companies lacked the capabilities to prioritize ITG mechanisms (i.e. IT processes) to be designed and implemented. This entailed the creation of informal implementation plans with low controllability. At the operational level, the governance model for all companies was based on reactive mechanisms (e.g. committees). Therefore, there was a lack of mechanisms to control the impact of decisions (monitoring, auditing, process execution).

Risk management, even when considered one of the most important dimensions both for researchers and practitioners, was commonly being ignored, or not considered as critical from a strategic perspective. The lack of business-IT alignment regarding risk management may have created different risk mitigation strategies that do not respond to the business' requirements. A formal and corporate risk aware culture was missing in all four companies. At the tactical level, the two local companies had identified IT risks and controls. The two multinational companies were missing a formally defined IT-RM portfolio. At the operational level, none companies had implemented control mechanisms to analyze cost-benefits on IT risks, to provide continuity plans, or to quantify IT risks and their propagation on business and IT assets.

We also found that value delivery was the most important dimension for all companies. Each of the companies had structures (i.e. committees) specifically dedicated to measuring the business value delivered by IT investments. Through periodical meetings and a formal process, the analyzed organizations monitored value delivery to achieve business-IT alignment and identify new IT investment opportunities. This is very important at the tactical level because it settles the foundation on how IT will support the business requirements and strategy. This can then be used by the IT department to identify critical IT services and assets, and to define controls that help mitigate risks over those IT resources. Even though the development of strategic level capabilities was expected to follow a top-down approach, some companies were capable to include those strategic capabilities leveraged by the already existing tactical and operational capabilities (on a bottom-up approach). All four companies would improve their value delivery at the operational level by incorporating capabilities to quantify non-financial value, to measure the value flow among IT architectures, and to forecast the value of IT assets.

Performance management was supported in all companies at the strategic level. This became evident through their clear definition of IT to support business strategy and through their periodical reports to the executive board regarding the performance of IT projects. However, at the tactical level, there were no agreements with the business units regarding the expected performance of IT nor was this performance measured. None of the companies performed periodic evaluations to determine if the utilization of IT assets (e.g. ROA), the rationalization of assets, or IT performance (profit, assets utilization, growth) were appropriate. At the operational level, all companies lacked the capabilities to control the utilization of inter-project or inter-process human resources and to monitor process performance.

5.3 Gap Analysis by Company

Gap analysis for the first multinational company (MC1)

Decisions were made by the International Headquarters (HQ) and then transmitted to the corresponding regional offices, where such decisions were adapted to a particular reality. Each regional office transmitted these decisions to the local subsidiaries in each country. As a result, the Colombian subsidiary had to comply with the global decisions.

Decision-making in this company was therefore constrained by the unified operational model of the organization (high standardization and integration of processes [3]). The organization had clearly defined decision-making structures and critical decisions to control. However, the interview data showed that the information was not as standardized as expected. This evidences the need for greater ITG efforts at the operational level in order to achieve more control. At a tactical level, the decision-making archetypes were not clearly identified for all decision types, especially because decisions were made by global or regional structures. There were formally defined service level agreements and the decisions were made only by the defined structures. However, this does not mean that the decisions were made by the right structure.

Risk management support at the strategic level was defined by the global HQ. Risk management in the Colombian subsidiary was focused on supporting project management but was not considered a mechanism to relate IT and corporate governance. Thus, risk management could be misdirected into different directions, causing misalignment between the business and IT. We noticed that risk management was a top priority for IT, but it was not considered important by the business. This explains the lack of a risk awareness culture in the Colombian subsidiary. To close this gap, the organization started implementing COBIT to identify the business impact on risk materialization. At the tactical level, there was not a formally defined IT risk management portfolio with detailed information of identified risks, IT assets and their vulnerabilities, nor was there any risk accountability. Finally, at the operational level, since no formal procedure of risk treatment was defined, the controls to treat the identified risk were implemented without a detailed cost-benefit analysis, and no IT audits were performed periodically to detect new vulnerabilities.

Value delivery was the most important dimension for this organization as declared by both the IT and business units. This was supported at the strategic level by a formal process to periodically measure and follow the business value delivered by IT, a regional committee to prioritize investments, and a budget approval committee for evaluating IT initiatives based on their Return On Investment (ROI). At a tactical level, the IT portfolio was periodically monitored to assure that the expected benefits were being transferred to the business, and periodic meetings were arranged to identify new IT investment. Finally, at the operational level, the organization had an IT portfolio with information regarding IT services, assets and investments. IT investments were implemented using project management methodologies. However, some business units considered that IT initiatives were not delivering as much business value as they could. This can be improved by incorporating communication mechanisms and by quantifying the non-financial value delivered by IT investments.

Performance management at the strategic level was well supported through a clear definition of IT for supporting business strategy while keeping the operation running. The executive board received periodical reports regarding the performance of IT projects. However, these expectations were no longer defined at the tactical and operational levels; there were no agreements with the business units regarding the expected IT performance, nor was this performance measured. Moreover, there were no periodic evaluations to determine if the utilization of IT assets was appropriate. Project metrics, such as the expected delivery time and the budget of IT projects, were missing resource utilization metrics to keep the project within the expected boundaries.

Gap analysis for the first local company (LC1)

This company behaved similarly to MC1 due to its clearly defined structures to make decisions. However, this organization did not define nor monitor agreements, something that generated conflicting decisions.

Even though this company had a risk awareness culture (risk management is critical for IT and the business), risk management was not considered as a mechanism to relate IT and corporate governance. As a result, risk management could be misdirected into different directions, causing misalignment between the business and IT. Risk appetite and tolerance were not formally defined. At the tactical level, IT risks on processes, controls, and initiatives were identified to improve the risk awareness culture. According to the data from the interviews, the performance of these initiatives was favorable throughout the entire organization. Consequently, the existing initiatives should leverage the formalization of risk management at a strategic level.

The capabilities of the value delivery dimension were not supported in this company. The prioritization of IT investments was performed by the board of directors and the budget was approved by the CEO and the CFO. Based on the data from the interviews, we identified a misalignment between the business and IT areas regarding value delivery. For example, IT did not consider it crucial that all IT initiatives delivered business value, despite this being a non-negotiable requirement for the business. The lack of a strategic support for value delivery may have caused this misalignment. A strategic approach regarding the measurement of business value delivered by IT is necessary in order to guarantee that all IT investments have a return.

Performance management at the strategic level evidenced a clear understanding of the expectations this business had concerning IT. The role of IT was exclusively operational (e.g. keeping the IT platform working, customer support). Therefore, the capabilities at tactical and operational levels were limited and no formal agreements or monitoring processes were defined. Moreover, despite the performance of IT services being measured in terms of platform availability and the organization not using standard project management methodologies, less than one project per year was delivered out of time or budget.

Gap analysis for the second multinational company (MC2)
Much like MC1, decision-making in MC2 was mainly supported by the international HQ and then transferred to a regional office and local subsidiaries, which lacked decision-making structures. The decision making archetypes at the corporate level were known throughout the organization as well as the conformation of the different committees making the decisions.

IT risk management evidenced the lack of a risk awareness culture from both, IT and the business, within the subsidiary (cf. risk awareness on IT in MC1). There was no alignment between the IT risk policy and the corporate risk policy. At the tactical level, there was no formally defined IT risk management. At the operational level, since no formal procedure of risk treatment was defined, the controls implemented to treat the identified risk were implemented without a detailed cost-benefit analysis, and no IT audits were performed periodically to detect new vulnerabilities.

Value delivery at the subsidiary had a formally established process to measure the business value delivered by IT, as well as a regional committee coordinated by the subsidiary to perform the prioritization of the investments. Furthermore, a budget approval committee, including the CEO and the CFO, ensured that all the approved IT initiatives had an associated ROI. At tactical and operational levels, the IT portfolio was periodically monitored to ensure that the expected benefits were being transferred to the business, and that periodic meetings were arranged to identify new IT investment opportunities that could better support the operation of the company. However, one of the findings that stems from analyzing this company is that value delivery from IT initiatives is not a priority for the business nor for IT. This could cause the company to spend resources on IT investments that do not deliver a return for the business.

Performance management at the strategic level constraints the IT role to keep the standards defined by HQ and to provide a good service for internal and external customers. At the tactical and operational levels, there were agreements with the business units regarding the expected performance and benefits of IT, but there were no formal evaluations of IT performance. There were no periodic evaluations to determine that the utilization of IT assets was appropriate either. Similarly to company LC1, performance of IT services was measured in terms of platform availability and customer satisfaction. Regarding customer satisfaction, the organization had results that indicated a score of 4 out of 5 in customer satisfaction concerning the IT services, which shows a good service level with opportunity for improvement.

Gap analysis for the second local company (LC2)

Despite the organization having defined structures to make decisions, decision-making responsibilities were not clearly defined. Moreover, at the tactical level, the decision making archetypes were not clearly identified because there was no detailed approach on who participated in each decision-making structure and, specifically, if there was any IT presence in the structures. The company had formally defined service level agreements and the decisions were made only by the defined structures.

Risk management was considered a mechanism that related IT and corporate governance, which helped to align the IT risk policy to the corporate risk policy, as well as to improve the risk-aware culture in the organization. This can be proved by reviewing the relative importance of risk management for both IT and the business. The company started working on the implementation of COBIT, and has focused on identifying the business impact of the materialization of an IT risk. At the tactical level, IT risk identification in the organization and prevention of risk materialization over business core processes had been implemented and monitored. At the operational level, there were no periodic IT audits to detect new vulnerabilities. Since there is a relation between IT and corporate risk policies, controls were defined based on a cost-benefit analysis.

The company had a formal process to measure the business value delivered by IT, which was carried out by the board of c-level executives. It also had a process to prioritize IT investments and a budget approval mechanism. Contrary to the other cases where the budget approval included either the CEO or the CFO, the person responsible for this approval was the purchase leader. This decision could be explained when considering that the purchase leader can get better prices from suppliers. At tactical and operational levels, the IT portfolio was periodically monitored to ensure that the expected benefits were being transferred to the business, and that periodic meetings were arranged to identify new IT investment opportunities that can better support the operation of the company. However, one of the metrics commonly used to identify value delivery, customer satisfaction with IT services, was not considered as critical for the business nor for IT. This induced the organization to spend resources on IT while disregarding the requirements and considerations of the customers, both internal and external.

Performance management included the IT role to provide technical solutions to business requirements and to comply with the guidelines defined by the organization. Customer satisfaction, peer review, and business process improvements were the critical metrics required to evaluate IT performance. As we mentioned before, at tactical and operational levels, customer satisfaction performance in this company was deficient for internal and external customers.

6 Conclusion

In this paper, we presented a set of capabilities for ITG practice at different levels (strategic, tactic, operational), according to the ITG academic literature, and classified them around the four dimensions of ITG. A similar exercise was then performed, but this time based on the ITG capabilities identified in four Colombian organizations of the logistics industry. The comparison between these two exercises allows us to conclude that there are indeed considerable gaps regarding the risk management dimension of ITG, as well as when considering the priorities assigned to the value delivery dimension. The bigger gaps are evident at an operational level.

One interesting finding is that even companies that used commercial frameworks like COBIT had significant gaps in their risk management dimension, something that could be read in one of two ways: (a) the importance of the IT risk management dimension is over-emphasized in the literature, or (b) practitioners see the recommendations of the ITG literature regarding IT risk management as an overkill and prefer a more relaxed approach. It is important to note, however, that this research does not intend to comment on the convenience of a robust and structured approach to IT risk management nor on the relaxed approaches assumed by the organizations in this research.

Finally, this research also supports the importance of considering the social aspects of ITG practices because, even though the interviewees talked very highly about the commercial frameworks used in their companies, most of them did not apply them fully and even went against the recommendations of such frameworks. This questions if the source of legitimacy of these frameworks is truly based on their technical value (a value that this research does not put into question) or if it is the result of political, social or marketing processes. These questions should be studied more carefully in future works about ITG.

References

1. Webb, P., Pollard, C., Ridley, G.: Attempting to define IT governance: wisdom or folly? In: Proceedings of the 39th Hawaii International Conference on System Sciences, pp. 1–10. IEEE (2006)
2. Brown, A., Grant, G.: Framing the frameworks: a review of IT governance research. Commun. Assoc. Inform. Sys. **15**, 696–712 (2005)
3. Weill, P.: Don't just lead, Govern: how top-performing firms govern IT. MIS Q. Exec. **3**(1), 1–17 (2004)

4. Giraldo O.L., Herrera, A., Gómez, J. E.: IT Governance State of Art at enterprises in the Colombian Pharmaceutical Industry. In: Quintela Varajão J.E., Cruz-Cunha M.M., Putnik G. D., Trigo A. (eds) ENTERprise Information Systems. CENTERIS 2010. CCIS, vol. 109. Springer, Berlin, Heidelberg
5. Jacobson, D.D.: Revisiting IT governance in the light of institutional theory. In: Proceedings of the 42nd Hawaii International Conference on System Sciences, pp. 1–9. IEEE (2009)
6. Willson, P., Pollard, C.: Exploring IT governance in theory and practice in a large multi-national organisation in Australia. Inform. Syst. Manage. **26**, 98–109 (2009)
7. Simonsson, M., Ekstedt, M.: Getting the priorities right: literature vs practice on IT governance. In: Technology Management for the Global Future—PICMET 2006 Conference, pp. 18–26. IEEE (2006)
8. Keyes-Pearce, S.: Rethinking the importance of IT governance in the e-World. In: Proceedings of the 6th Pacific Asia Conference on Information Systems, pp. 256–272. AISeL (2002)
9. Winkler, T., Brown, C.V.: Horizontal allocation of decision rights for on-premise applications and software-as-a-service. J. Manage. Inform. Syst. **30**, 13–48 (2014)
10. Ko, D., Fink, D.: Information technology governance: an evaluation of the theory-practice gap. Corp. Govern. **10**, 662–674 (2010)
11. Winkler, T., Goebel, C., Benlian, A., Bidault, F., Günther, O.: The impact of software as a service on IS authority—a contingency perspective. In: Proceedings of the 32nd International Conference on Information Systems, pp. 1–17. AISeL (2011)
12. Yin, R.K.: Case Study Research: Design and Methods. Sage Publications, Thousand Oaks (2008)
13. Ulrich, W., Rosen, M.: The business capability map: the “rosetta stone” of business/IT alignment. Enterp. Archit. **14** (2011)
14. Eisenhardt, K.M., Martin, J.A.: Dynamic capabilities: what are they? Strateg. Manage. J. **21**, 1105–1121 (2000)
15. Swauger, J.: Is it time for an IT governance audit? EDPACS **47**, 1–6 (2013)
16. González-Rojas, O., Lesmes, S.: GovernIT: a software for decision-making support on automated IT governance models. In: Information Systems Development: Advances in Methods, Tools and Management (ISD2017 Proceedings), pp. 12. AISeL (2017)
17. Westerman, G., Hunter, R.: IT Risk: Turning Business Threats Into Competitive Advantage. Harvard Business School Press, Boston, MA, USA (2007)
18. ISACA: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA (2012)
19. Cervone, F.: ITIL: a framework for managing digital library services. Digit. Libr. Perspect. **24**, 87–90 (2008)
20. Fonstad, N.O., Robertson, D.: Transforming a company, project by project: the IT engagement model. MIS Q. Exec. **5**, 1–14 (2006)
21. Heart, T., Maoz, H., Pliskin, N.: From governance to adaptability: the mediating effect of IT executives’ managerial capabilities. Inform. Syst. Manage. **27**, 42–60 (2010)
22. Gonzalez-Rojas, O., Beltrán, G., Correal, D.: Measurement of current and potential non-financial business value delivery of IT investments. Information **19**, 2869–2874 (2016)
23. Kohnke, A., Shoemaker, D.: Making cybersecurity effective: the five governing principles for implementing practical IT governance and control. EDPACS **52**, 9–17 (2015)
24. ISO: ISO/IEC 38500;2008: Corporate Governance of Information Technology. International Standards Organisation (2008)
25. Jordan, E.: An integrated IT risk model. In: Proceedings of the 9th Pacific Asia Conference on Information Systems: IT & Value Creation, pp. 632–644. AISeL (2005)
26. Caralli, R., Stevens, J., Young, L., Wilson, W.: Introducing OCTAVE Allegro: improving the information security risk assessment process (No. CMU/SEI-2007-TR-012) (2007)
27. Héroux, S., Fortin, A.: Exploring IT dependence and IT governance. Inform. Syst. Manage. **31**, 143–166 (2014)

28. González-Rojas, O.: Governing IT services for quantifying business impact. In: Matulevicius, R., Dumas, M. (eds.) Perspectives in Business Informatics Research. BIR 2015. LNBIP, vol. 229, pp. 97–112. Springer, Cham (2015)
29. González-Rojas, O., Lesmes, S.: Value at risk within business processes: an automated IT risk governance approach. In: La Rosa, M., Loos, P., and Pastor, O. (eds.) Business Process Management. BPM 2016. LNCS, vol. 9850, pp. 365–380. Springer, Cham (2016)