Identifying Gaps on IT Governance Capabilities: Findings in the Logistics and Transportation Industry in Colombia

Oscar González-Rojas *o-gonza1@uniandes.edu.co*
Systems and Computing Engineering Department
Universidad de los Andes
Bogotá, Colombia

Juan E. Gómez-Morantes *juan.gomezmorantes@manchester.ac.uk*
Global Development Institute
University of Manchester
Manchester, UK

Guillermo Beltrán *ga.beltran66@uniandes.edu.co*
Systems and Computing Engineering Department
Universidad de los Andes
Bogotá, Colombia

Abstract

Nowadays, Information Technology (IT) governance is a core activity adopted or 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 these capabilities in the practice of Colombian companies within the logistic industry. The main gaps on adopting IT governance capabilities are discussed and research insights are provided for aligning theory and practice.

Keywords: ICT governance, capability model, business ICT alignment, risk management.

1. Introduction

Initially considered as a sub-set of corporate governance, IT Governance (ITG) has emerge as its own discipline since the 90s [21]. Although it was not until the late 90s when the term ITG gained traction in the literature, it is possible to find similar concepts as early as 1963 [1]. Later, in the mid-2000s, evidence about the link between ITG and performance in big organizations [22] generated great interest in both academics and practitioners. Since then, a large body of literature has been published looking at 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, and prescriptive models of ITG implementations [13], [24].

While the aforementioned stream of research has provided 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 Section 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. Furthermore, a wider empirical base will allow for ITG research to be better informed by actual ITG practice; something that is essential to close the theory-practice gap discussed in this paper.

[1] More than 30.000 publications can found in Google Scholar using the query “IT Governance”

The remainder of this paper is as follows. In Section 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. Therefore, we present the identified gaps and a characterization of the capabilities of this industry. Finally, conclusions and future work are presented in Section 6.

2. IT Governance: Context, Issues, and Gaps

As a result of the more than two decades of research in the subject, it is possible to find multiple definitions of ITG proposed from different perspectives and with different focuses and objectives [18], [21]. From a more practice-focused perspective, plenty of literature exists covering ITG frameworks, implementation processes, and good practices. This is a difficult issue in the field because the lack of consensus in the very definition of the concept within the academic community hinders the advancement of the field. Furthermore, the lack of consensus on this definition between academics and practitioners hinders the communication between these groups, and reduces the chances of collaboration between them [15].

The issue of the multiple ITG definitions has been debated in recent literature [1], [21]. It is now commonly accepted that the core of ITG is composed by four dimensions: (a) organizational structures for 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 indicated by Weill, “IT Governance is not about what specific decisions are made. That is management” [22]. This means that ITG is about the specification and implementation of organizational structures and processes 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 with time, and also 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 like cloud computing are challenging our current knowledge about ITG and how it is performed [25].

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 relayed to 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)” [13]. The biggest issue with the over-reliance on these rational theories is that they are not well equipped to understand some of the more social aspects of ITG like 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 with 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 the ITG literature, one of the most relevant gaps is the theory-practice 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 lack of knowledge from practitioners, as even when fairly familiar with the literature, practitioners 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 practitioner can inform the literature and open new research avenues.

These gaps between ITG definitions and representations have been discussed and researched by multiple authors. Keyes-Pearce [15] 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 founds that the motivations for the adoption of ITG models diverge from the "IT as a source of competitive advantage" discourse pushed by the literature and is closer to a more pragmatic "IT as a competitive necessity". Additionally, the author found that practitioners are often unable to articulate what ITG means for them. Ko and Fink [16] studied gaps in three dimensions of ITG: structures, people, and processes. Although no definition of gap is given, it can be inferred that they understands 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 [18] 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 although there are no major differences in the priorities of these groups, there are some differences in the priorities assigned by them. The main findings are that practitioners tend to give more priority to the understanding phase of the decision making process, while the literature give more importance to the monitoring phase of the process. Also, practitioners assign less importance to tactical issues than the literature.

Willson and Pollar [24] present an in-depth study of ITG practices in a large Australian multinational organization. In this case, the authors found practices not currently covered in the ITG literature like performance measuring as a tool in ITG. Furthermore, and perhaps more important, the authors found factors like organizational history and nature that have significant impact on ITG models and practices. This case, then, is instrumental in arguing that there is a lot that the academic literature can learn from studying actual ITG practices. Finally, Winkler et al. [26] explored the impacts of new technology models like the Software as a Service (SaaS) on current ITG practices, focusing on the structural elements of ITG.

In summary, the theory-practice gaps currently studied in the literature can be classified using three categories; ontological gaps, ITG antecedents' gaps, and dynamic gaps. The ontological gaps make reference to differences on what ITG is, how is ITG performed, and what factors are important in ITG practice. The antecedents gaps refers to the importance of ITG, the business imperative of ITG efforts, and the priorities on ITG practices vs the perspectives expressed by the literature. Finally, dynamic gaps make reference to the lack of literature on change and evolution of governance practices.

3. Research Methodology

To contribute to the better understanding of theory-practice gaps in ITG, the main research question of this paper is: *RQ: 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 highly detailed information to measure gaps between theory and practice in ITG, this paper follows a qualitative approach based on the case study method. The case studies follow a multiple-case design with embedded units of analysis [27] to introduce an element of triangulation at the empirical level and to improve the veracity of the findings. The embedded units of analysis are the four dimensions of ITG identified in Section 2.

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 analyzed exclusively the Colombian subsidiary of multinational companies. The companies' size ranges from 800 to 3000 employees.

One to three in-depth interviews with high ranking managers (e.g. CIO, CEO) were performed in for each case. The interviews followed a semi-structured model based on a survey of 49 questions.[2] We designed this questionnaire around the four embedded units of analysis by uncovering 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 Section 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 looks to highlight areas for evaluating and researching existing ITG theory-practice gaps. The data gathered in the interviews is used to build a profile of the ITG practices for each company. These profiles are then compared to the capabilities model and a gap analysis is 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. The first limitation is that it only includes Colombian companies from the logistics industry. Since ITG issues are highly contingent (i.e. they depend on the context), the data and conclusions presented in this research could differ from the reality of other regions or other industries. The second limitation is related with the methodology used for 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 intent to achieve generalizability to populations but to theoretical elements. This means that the value of this research is not in any predictive or prescriptive statement, but in the ITG capability model presented in section 4 as a tool to evaluate ITG theory-practice gaps.

4. Core Capabilities on IT Governance

A *Capability* is a particular ability owned by an organization or system to achieve a specific goal [20]. These abilities are enabled by a combination of resources (e.g. people, processes, IT) and by how those resources are managed [4]. Therefore, the application of IT governance capabilities and their continuous improvement and evolution over time can differentiate the companies within a particular industry.

We created a capabilities model by aggregating different sources of information regarding ITG. These capabilities were grouped in four dimensions (decision-making, risk management [19], value delivery and alignment, and performance management [19]) and then characterized into three levels (strategic, tactical and operational capabilities).

Strategic capabilities refer to high-level decisions-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 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 [22]. Table 2 describes the actions and capabilities identified for the value delivery and alignment dimension. This dimension is focused on using IT investment as linkages between company-wide ITG, business unit levels and project team level, both for business and IT. These linkages will represent value to the organization as a whole [5].

[2] The designed survey is available on:
https://github.com/governit/ITG_LogisticsIndustry/blob/master/Survey_EN.pdf

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

	Action (WHAT)	Capabilities (HOW)
Strategic	1. Establish desired IT behavior [22] 2. Establish decision accountability on IT Principles, Enterprise Architecture, Business Application Needs, IT Infrastructure, IT Investment and prioritization [22] 3. Establish input rights on decisions [22] 4. Identify archetypes per decision type (e.g. Monarchy, Federal, IT Duopoly, Feudal) [22]	**Structures** 1. Committees (Executive committee, IT leaders Committee, Process Team, Account managers) [22] **Information/Artefacts/Resources** 2. Decision maps per delegation of authority (accountabilities) and archetype [22] 3. Politics for exception handling [22] 4. Internal communication mechanisms (e.g. web portals) [22]
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)	**Processes** 1. Coaching to stakeholders that are not following decision rules [22] **Information/Artefacts/Resources** 2. Agreement definition (SLA, OLA, UC) [22] 3. Definition of target decision maps 4. Coaching to stakeholders not following decision rules [22] **Communication** 5. Managerial alerts [22]
Operational	1. Define control on decision making [22] 2. Specialize generic decisions within the five strategic decision categories	**Processes** 1. Audit procedures [23] 2. Measurement on assets utilization – COBIT EDM04 Ensure resource optimization [11] 3. Monitoring of agreements - COBIT APO09 Manage service agreements [11] 4. Processes on IT frameworks (e.g. COBIT [11], ITIL [3]) **Information/Artefacts/Resources** 5. IT Metrics regarding decision rights [22]

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

	Action (WHAT)	Capabilities (HOW)
Strategic	1. Establish guidelines of value delivery measure [11] 2. Prioritize investment initiatives based on clearly defined criteria (e.g. higher benefits, less risk) [11], [22]	**Structures** 1. Board of directors [11] 2. Management Committee [11] 3. Project Management Office (PMO) [11] 4. IT executives with deep understanding of business environment [9] **Processes** 5. Project management [11]
Tactical	1. Manage IT value generation and delivery [11] 2. Identify opportunities of IT portfolio improvement [11] 3. Prioritize new IT investments and projects [11] 4. Evaluate IT portfolio distribution after organizational changes [11]	**Structures** 1. Project Management Office (PMO) [11] **Processes** 2. Definition of metrics of non-financial value [11] 3. Quantification of non-financial metrics [7] 4. Processes of IT investment portfolio management – COBIT process BAI01 Manage Programmes and projects [11] **Information/Artefacts/Resources** 5. Financial value metrics (e.g. ROA, ROI, ROE, NPV) [22] 6. Ratio between IT operation costs and obtained benefits [11]
Operational	1. Evaluate benefits generated by IT services, assets and investments define don IT portfolio [11] 2. Implement new IT investments and projects following a project management methodology [11] 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 [11] 2. Calculation of the financial value delivered to the business, regarding IT services behavior (risks, service agreements, costs, income, and alignment) **Information/Artefacts/Resources** 3. Metrics by asset [11] 4. Project management methodology [11] 5. Value flow measurement techniques

Table 3 describes the core actions and capabilities identified regarding risk management on ITG. Risk management covers the unplanned events that may represent a failure in IT and that will threaten enterprise goals, due to IT pervasiveness [23]. 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 [11].

Table 3. Actions and capabilities to support the risk management dimension.

	Action (WHAT)	Capabilities (HOW)
Strategic	1. Plan and direct risk management [17] 2. Align IT risk policy with corporate risk policy [11] 3. Build a risk-aware culture [23] 4. Define and implement a risk governance process [23]	**Structures** 1. Executive level (Board of directors, management committee) [11], [23] **Information/Artefacts/Resources** 2. Risks map 3. Risk appetite and tolerance [11] **Processes** 4. COBIT Process EDM03- Ensure Risk Optimization [11] 5. List of breaches that executives could be accountable for [12] 6. Segmented audiences based on their role towards risk awareness [23]
Tactical	1. Assess IT-related risks that may affect the organization [11] 2. Create and maintain an IT risk management portfolio [14] 3. Align IT risk management with corporate risk management	**Structures** 1. Management committee [22] 2. IT specialized committees [22] **Processes** 3. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation) processes for assess risks on Information Security [2] 4. Risk policies and standards [17] 5. COBIT process APO12- Manage Risks (Create and maintain a formal document with the identified risks) [11] **Communication** 6. COBIT process EDM03.02 (Channels to deliver the campaigns to all the employees) [11]
Operational	1. Collect and analyze information regarding IT risks [23] 2. Perform a cost-benefit analysis on risks [23] 3. Design and prove a business continuity plan [23] 4. Identify and close vulnerabilities in the IT assets base [23] 5. Implement controls and industry best practices [11] 6. Simulate solution scenarios to control risks 7. Report risks materialization [11]	**Structures** 1. Service manager [11] 2. Business-IT Council [22] 3. IT specialized committees [22] 4. IT Audit [10], [22], [23] **Processes** 5. COBIT process APO12.01 - Manage Risks [11] 6. Risk quantification of operational assets (processes, IT services) [6], [8] 7. Business Impact Analysis (BIA) [23] 8. Business continuity plan with responsible and expected quality of service levels [23] 9. IT audits [10] 10. COBIT process APO12.02 (Cost-benefit analysis on risks treatment) [11] **Information/Artefacts/Resources** 10. List of critical IT assets and their vulnerabilities [2] 11. Test environments [11] **Communication** 12. Channels to notify materialization of a risk to the person responsible

Table 2. 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 [11] 2. Manage the use of IT resources	**Structures** 1. Executive committee [11], [22] 2. IT specialized committees [22] **Processes** 3. Models of IT agreements or contracts [11] 4. Measurement of resources use (time, costs) [11]
Tactical	1. Specify agreements with the stakeholders regarding performance goals and metrics expected from IT [11] 2. Rationalize asset use 3. Evaluate IT performance on profit, asset utilization, growth [22]	**Structures** 1. Management committee [22] **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 and identify improvement opportunities 2. Manage IT assets [11] 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 [11]	**Processes** 1. COBIT process MEA01-Monitor and evaluate performance and conformance [11] 2. COBIT process BAI09-Manage Assets [11] 3. COBIT process APO07-Manage human resources [11] **Information/Artefacts/Resources** 4. Map of IT assets and corporate processes supported by those assets [11] 5. IT portfolio [11]

5. Measuring Gaps on IT Governance Capabilities

Table 5 describes how the capabilities defined on Section 4 can be evaluated in terms of two elements: existence and function. This means that is not enough to have an ITG structure, this structure has to perform certain tasks to consider that the organization has the capability. Based on this analysis, this section presents the most significant theory-practice gaps identified after evaluating ITG capabilities on the four companies mentioned in Section 3.

At the end of this analysis we identified an approach that can be used as a characterization of the sector. First of all, risk management, even when considered one of the most important dimensions both for researchers and practitioners is commonly being ignored, or not considered as critical from a strategic perspective. The lack of business-IT alignment regarding risk management may create risk mitigation strategies that do not respond the business requirements.

We also found that value delivery is the most important dimension. Companies had structures dedicated specifically to measure business value delivered by IT investments. Through the value delivery definition and monitor, organizations achieve business-IT alignment. This is very important because it settles the foundation on how IT will support the business requirements and strategy. This is then used by the IT department to identify critical IT services and assets and to define controls to mitigate risks over those IT resources.

This also explains why some companies have developed tactical or operational capabilities without a strategic definition (since the development of capabilities was expected to be from a top-down approach), and are capable to include those strategic capabilities leveraged by those already existing tactical and operational capabilities (on a bottom-up approach).

Table 3. Expected evidence on IT governance capabilities.

	Strategic	Tactical	Operational
Decision-Making support	DS1. Decisions are explicit DS2. Decision-making structures (e.g. committees) 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 the expected IT behavior	DT1. Decision-making archetypes are defined and recognized for each of decision types 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 made them	DO1. All decisions are clearly identified and classified into one of the five decision types DO2. Governance model is based on proactive over reactive mechanisms DO3. Defined agreements are monitored periodically using technical tools
Risk Management	RS1. There is an organizational risk aware 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 among the organization	RT1. IT risks that may affect the organization are clearly identified and assessed RT2. There is a formal definition of IT risk owners and IT risk management responsible RT3. There is an IT risk management portfolio that collects the information of the identified risks	RO1. Cost-benefit analysis are performed periodically on IT risks RO2. A business continuity plan is defined and tested periodically RO3. Controls over IT risks are implemented based on cost-benefits 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 monitored constantly to assure benefits transfer VT2. Continuous analysis of investment opportunities to improve the IT portfolio VT3. New IT investment initiatives are prioritized based on organizational criteria VT4. IT portfolio is reviewed periodically to keep it updated with organizational changes	VO1. There is an IT portfolio with information of IT services, assets and investments VO2. IT investment and projects follow project management methodologies VO3. The business value delivery from IT services is quantified
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 the performance of IT	PO1. IT services are evaluated against stakeholders' expectations PO2. IT assets are evaluated periodically to guarantee that they are used effectively to support business requirements PO3. Human resources are used effectively to support multiple business processes

Gap analysis for the first multinational company (MC1)

Decisions are made by the International Headquarters (HQ) and then transferred to regional offices to adapt them to their reality. Each regional office transfers decisions to the local subsidiaries of each country. The Colombian subsidiary has to comply with the global definitions.

Decision-making is constrained by the unification operational model of the organization (high standardization and integration of processes [22]). The organization has clearly defined decision making structures and decisions. However, the interview data showed that the information is not standardized as expected. This evidences the need for more ITG efforts at the operational level to achieve more control. At a tactical level, the decision making archetypes are not clearly identified for all decision types, especially when the decisions are made by global or regional structures. There are formally defined service level agreements and the decisions are made only by the defined structures. However, this does not mean that the decisions are being made by the right structure.

Risk management at the strategic level is defined by the global HQ. Risk management in the Colombian subsidiary is focused on supporting project management but is not considered as a mechanism relating IT and corporate governance. Thus, risk management can be administered into different directions, causing misalignment between business and IT. We identified that risk management is a top priority for IT, but is not considered important by business. This explains the lack of risk awareness culture in the Colombian subsidiary. To close this gap, the organization is implementing COBIT for identifying the business impact on risks materialization. At the tactical level, there is not a formally defined IT portfolio with detailed information of identified risks, IT assets and its vulnerabilities, and accountability of risks. Finally, at the operational level, since no formal procedure of risk treatment is defined, the controls implemented to treat the identified risk are implemented without a detailed cost-benefit analysis, and no IT audits are performed periodically to detect new vulnerabilities.

Value delivery is the most important dimension for this organization as declared by both IT and business units. This is 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 ROI. At tactical level, the IT portfolio is monitored periodically to assure that the expected benefits are being transferred to the business, and periodic meetings are made to identify new IT investment. Finally, at the operational level, the organization has an IT portfolio with information regarding IT services, assets and investments. IT investments are implemented using project management methodologies. However, some business units consider that IT initiatives are 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 is well supported by the clear definition of IT for supporting business strategy while keeping the operation running. The executive board receives periodical reports regarding the performance of IT projects. However, at the tactical and operational level these expectations are no longer defined; there are no agreements with the business units regarding the expected performance IT, nor this performance is measured. Moreover, there are not periodic evaluations to determine that the utilization of IT assets is appropriate. Projects metrics such as the expected delivery time and the budget of IT projects are missing resource utilization metrics to keep project within the expected boundaries.

Gap analysis for the first local company (LC1)

This company behaves similarly to MC1 by having clearly defined structures to make decisions. However, the organization does not define nor monitor agreements, something that generates conflicting decisions. This company has a risk aware culture (risk management is critical for IT and the business). However, risk management is not considered as a mechanism relating IT and corporate governance. Thus, risk management can be administered into different directions, causing misalignment between business and IT. Risk appetite and tolerance are not formally defined. At the tactical level, IT risks on processes, controls, and initiatives are identified to improve the risk aware culture. According to the interview data, the performance of these initiatives is widely favorable among all the organization. The existing initiatives should leverage the formalization of risk management at a strategic level.

The capabilities of the value delivery dimension are not supported in this company. The prioritization of IT investments is performed by the board of directors and the budget is approved by the CEO and CFO. From the interview data we identified a misalignment between the business and IT areas regarding value delivery. For example, IT did not consider fundamental that all IT initiatives deliver business value, while for the business this is a non-negotiable requirement. Lacking a strategic support for value delivery is what may cause this misalignment. A strategic approach regarding the measurement of business value delivered by IT is necessary to guarantee that all IT investments will indeed have a return.

Performance management at the strategic level evidences a clear understanding of the expectations the business has on IT. The role of IT is exclusively operational (keep the IT platform working, customers support). This constraint the capabilities on tactical and operational levels since no formal agreements or monitoring processes are defined. The performance of IT services is measured in terms of availability of the platform. In contrast, less than one project per year is delivered out of time or budget even though the organization does not use standard project management methodologies.

Gap analysis for the second multinational company (MC2)

Similar to MC1, decision-making is mainly supported by the international HQ and then transferred to a regional office and local subsidiaries which lack decision-making structures. The decision making archetypes at the corporate level are known in the organization and the conformation of the different committees making the decisions is known.

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

Value delivery at the subsidiary has 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. It also has a budget approval committee including the CEO and the CFO, to assure that all the IT initiatives approved have associated a return on the investment. At tactical and operational level, the IT portfolio is monitored periodically to assure that the expected benefits are being transferred to the business, and periodic meetings are made to identify new IT investment opportunities that can better support the operation of the company. However, we found that value delivery from IT initiatives is not a priority neither for the business nor for IT. This may cause the company to spend resources on IT investments that do not deliver a return for the business.

Performance management at the strategic level scopes 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 level there are agreements with the business units regarding the expected performance and benefits of IT, but no formal evaluations of the performance of IT. There are no periodic evaluations to determine that the utilization of IT assets is appropriate. Similar to company LC1, performance of IT services is measured in terms of availability of the platform and by customer satisfaction. Regarding customer satisfaction, the organization has results that indicated a 4 over 5 in customer satisfaction with IT services, showing a good service level with some improvement opportunity.

Gap analysis for the second local company (LC2)

Despite the organization has defined structures to make decisions, decision-making responsibilities are not clearly defined because there is no detailed approach on who are the participants on each decision-making structure and specifically if there is IT presence in the structures. There are formally defined service level agreements and the decisions are made only by the defined structures.

Risk management is considered as a mechanism relating IT and corporate governance, which helps 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 both for IT and for the business. The company is working in the implementation of COBIT, focusing on identifying the business impact of the materialization of an IT risk. At the tactical level, IT risk identification in the organization and the prevention of risk materialization over business core processes are implemented and monitored. At the operational level, there are no periodic IT audits to detect new vulnerabilities. Since there is a relation between IT and corporate risk policies, controls are defined based on cost-benefit analysis.

The company has a formal process to measure the business value delivered by IT performed by the board of c-level executives. It also has a process of prioritization of IT investment and a budget approval mechanism. Contrary to the other cases where the budget approval included either the CEO or the CFO, the responsible of this approval is the purchase leader. This decision may be explained considering that the purchase leader can get better prices with the providers. At tactical and operational level, the IT portfolio is monitored periodically to assure that the expected benefits are being transferred to the business, and periodic meetings are made to identify new IT investment opportunities that can better support the operation of the company. However, one of the metrics commonly used to identify the value delivery, customer satisfaction with IT services, is not considered as critical neither for the business nor for IT. This induces the organization to spend resources on IT disregarding the requirements and considerations of the customers, both internal and external.

Performance management includes 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 are the critical metrics that are required to evaluate IT performance. At a tactical and operational level, as mentioned before, customer satisfaction performance is deficient for internal and external customers.

6. Conclusion

This paper presented a set of capabilities for ITG practice at different levels (strategic, tactic, operational) according to ITG academic literature, classifying them around the four dimensions of ITG. A similar exercise is then performed, but this time based on the ITG capabilities identified in 4 Colombian organizations of the logistics industry. A comparison between these two exercises concluded that there are indeed considerable gaps in the risk management dimension of ITG, as well on the priorities assigned to the value delivery dimension. The bigger gaps are evident at the operational level.

One interesting finding was that even companies that used commercial frameworks like COBIT had important holes in their risk management dimension, something that could be read in one of two ways: (a) the importance of 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 decide for a more relaxed approach. It is important to note, however, that this research does not intent to comment on the convenience of a robust and structured approach to IT risk management or the relaxed approaches assumed by the organizations in this research.

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

References

1. Brown, A., Grant, G.: Framing the Frameworks: A Review of IT Governance Research. Commun. Assoc. Inform. Sys. 15, 696–712 (2005)
2. 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)
3. Cervone, F.: ITIL: A Framework for Managing Digital Library Services. Digit. Libr. Perspect. 24 (2), 87–90 (2008)
4. Eisenhardt, K.M., Martin, J.A.: Dynamic Capabilities: What are They? Strateg. Manage. J. 21 (10–11), 1105–1121 (2000)

5. Fonstad, N.O., Robertson, D.: Transforming a Company, Project by Project: The IT Engagement Model. MIS Q. Exec. 5 (1), 1–14 (2006)
6. González-Rojas, O.: Governing IT Services for Quantifying Business Impact. In: Matulevicius, R. and Dumas, M. (eds.) Perspectives in Business Informatics Research. BIR 2015. LNBIP 229, pp. 97-112. Springer, Cham (2015)
7. Gonzalez-Rojas, O., Beltrán, G., Correal, D.: Measurement of Current and Potential Non-Financial Business Value Delivery of IT Investments. Inform. 19 (7B), 2869–2874 (2016)
8. 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 9850, pp. 365-380. Springer, Cham (2016)
9. Heart, T., Maoz, H., Pliskin, N.: From Governance to Adaptability: The Mediating Effect of IT Executives' Managerial Capabilities. Inform. Syst. Manage. 27 (1), 42–60 (2010)
10. Héroux, S., Fortin, A.: Exploring IT Dependence and IT Governance. Inform. Syst. Manage. 31 (2), 143–166 (2014)
11. ISACA: COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. ISACA (2012)
12. ISO: ISO/IEC 38500;2008: Corporate governance of information technology. International Standards Organisation (2008)
13. Jacobson, D.D.: Revisiting IT Governance in the Light of Institutional Theory. In: 42nd Hawaii International Conference on System Sciences, pp. 1–9. IEEE (2009)
14. Jordan, E.: An Integrated IT Risk Model. In: 9th Pacific Asia Conference on Information Systems: IT & value creation, pp. 632–644. AISeL (2005)
15. Keyes-Pearce, S.: Rethinking the Importance of IT Governance in the e-World. In: 6th Pacific Asia Conference on Information Systems, pp. 256–272. AISeL (2002)
16. Ko, D., Fink, D.: Information Technology Governance: An Evaluation of the Theory-practice Gap. Corp. Govern. 10 (5), 662–674 (2010)
17. Kohnke, A., Shoemaker, D.: Making Cybersecurity Effective: The Five Governing Principles for Implementing Practical IT Governance and Control. EDPACS 52 (3), 9–17 (2015)
18. Simonsson, M., Ekstedt, M.: Getting the Priorities Right: Literature vs Practice on IT Governance. In: Technology Management for the Global Future, pp. 18–26. IEEE (2006)
19. Swauger, J.: Is it Time for an IT Governance Audit?. EDPACS 47 (3), 1–6 (2013)
20. Ulrich, W., Rosen, M.: The Business Capability Map: The "Rosetta Stone" of Business/IT Alignment. Enterprise Architecture 14 (2), (2011)
21. Webb, P., Pollard, C., Ridley, G.: Attempting to Define IT Governance: Wisdom or Folly? In: 39th Hawaii International Conference on System Sciences, pp. 1–10. IEEE (2006)
22. Weill, P.: Don't Just Lead, Govern: How Top-Performing Firms Govern IT. MIS Q. Exec. 3 (1), 1–17 (2004)
23. Westerman, G., Hunter, R.: IT Risk: Turning Business Threats Into Competitive Advantage. Harvard Business School Press, Boston, MA, USA (2007)
24. Willson, P., Pollard, C.: Exploring IT Governance in Theory and Practice in a Large Multi-National Organisation in Australia. Inform. Syst. Manage. 26 (2), 98–109 (2009)
25. Winkler, T., Brown, C.V.: Horizontal Allocation of Decision Rights for On-Premise Applications and Software-as-a-Service. J. Manage. Inform. Syst. 30 (3), 13–48 (2014)
26. Winkler, T., Goebel, C., Benlian, A., Bidault, F., Günther, O.: The Impact of Software as a Service on IS Authority – A Contingency Perspective. In: 32nd International Conference on Information Systems. pp. 1–17. AISeL (2011)
27. Yin, R.K.: Case Study Research: Design and Methods. Sage Publications (2008)