

Article

Best Practices Kits for the ICT Governance Process within the Secretariat of State-Owned Companies of Brazil and Regarding these Public Companies

Edna Dias Canedo ^{1,*}, Ruyther Parente da Costa ^{1,†}, Rafael Timóteo de Sousa Junior ^{2,†}
and Georges Daniel Amvame Nze ^{2,†}

¹ Computer Science Department, University of Brasília (UnB), P.O. Box 4466, Brasília-DF CEP 70910-900, Brazil; ruyther@me.com

² Cybersecurity INCT, Decision Technologies Laboratory—LATITUDE, Electrical Engineering Department (ENE), Technology College, University of Brasília (UnB), Brasília-DF CEP 70910-900, Brazil; desousa@unb.br (R.T.d.S.J.); georges@unb.br (G.D.A.N.)

* Correspondence: ednacanedo@unb.br; Tel.: +55-61-98114-0478

† These authors contributed equally to this work.

Received: 17 April 2018; Accepted: 5 June 2018; Published: 9 June 2018



Abstract: This article introduces an Information and Communication Technology Governance Kit to be used by the Brazilian Secretariat of Coordination and Governance of State Enterprises (in Portuguese, Secretaria de Coordenação e Governança das Empresas Estatais—SEST) in regards to its governed companies. The proposed kit is an instrument of targeting, which presents a set of best practices and conditioning aimed at the development and implementation of improvements in the management of ICT resources by Brazilian state-owned companies that are controlled by SEST. The proposed kit comprises three situation scenarios and four maturity levels. For each proposed process, the artifacts and templates are presented for the controlled companies to implement their respective processes so that these companies guide the improvements in their ICT governance maturity level. Considering that SEST is the principal entity in this governance structure, the main contribution of the proposed kits is to facilitate, guide and improve the maturity level of all Brazilian state-owned enterprises.

Keywords: ICT governance; best practices; conditioning factors; implementation of ICT governance practices; Brazilian state-owned companies

1. Introduction

Information and Communications Technology (ICT) has become a fundamental element in the operations and strategies of organizations. This only reinforces the concern with practices capable of reducing operating risks and guaranteeing the continuity of the services offered to society. ICT has become widespread in the present business scenario, which is dynamic and very often prone to turbulence. In the past, executives could delegate, ignore or even postpone decisions on ICT [1]. This is no longer possible today, particularly in the majority of the bodies in the Brazilian Federal Public Administration (in Portuguese, Administração Pública Federal—APF), due to a high dependence of organizations on ICT, something that produces greater vulnerabilities, as inherently found in ICT environments.

In the present scenario, ICT has changed in the effort to cater to the needs of increasingly complex business environments, dealing with a diversity of automation and integration cases. Keeping ICT in line with the business is still a major challenge for organizations, as well as constantly adding value to it. ICT has the potential not only to support existing business strategies, but also to lead to new ones.

Along this line, it is not only a factor for survival and prosperity, but also an opportunity to throw into relief and simultaneously attain a good performance [1].

A major issue related to ICT is how to use it in a manner that is in line with the business, to obtain better results. The mere preparation of a model for ICT governance does not necessarily mean that a manner of ICT governance is actually in place, given that when governance processes are poorly designed and are out of date, they end up not being efficient.

Brazilian federal state-owned enterprises have different forms of organization, management and personnel policies and achieve different results, both operational and related to public policies in which they are inserted. These different systems, among other reasons, such as the size of the companies and the diversity of sectors in which they operate, make it difficult to follow up on their management and to identify improvement points.

It becomes strategic to allow the Brazilian state to act in a coordinated manner, directed by the Brazilian Secretariat of Coordination and Governance of State Enterprises (in Portuguese, Secretaria de Coordenação e Governança das Empresas Estatais—SEST), seeking greater uniformity of governance, structure and policies. It is also important to provide governance guided and accompanied by the Representatives of Shareholders and to act in accordance with the best governance practices identified by them or in the market. These strategic guidelines support SEST to achieve the desired results and improve the public services provided.

In this context, as described in this paper, SEST is proposing best practice kits for Information and Communication Technology Governance (ICT Governance) to be used as guidelines by the federal state companies in the evolution of their Information and Communication Technology Governance Systems (ICTGS). The ICT Governance Kits consist of sets of practices related to the governance of ICT, the ICT governance model that is suggested to these state enterprises, to develop and refine their ICT governance.

The proposed practices are related to the role of the company under governance regarding the optimization of its ICT resources in its activities. Each practice described in this paper has been associated with a set of conditions and artifacts, which represent the internal and/or external factors that impact its execution, within the organizational context.

Each proposed kit comprises an instrument of targeting and a set of practices and conditioning aimed at developing and implementing improvements in state enterprises through the proposed model. The ICT Governance Kit is the result of a collaborative process for proposing Information and Communication Technology Governance best practices, which involved members of SEST and the University of Brasília (UnB).

The challenge of SEST includes establishing a road-map to applying the ICT Governance recommendations issued by the Brazilian Federal Court of Accounts (in Portuguese, Tribunal de Contas da União—TCU) or to checking the adherence to these recommendations. In this sense, this paper introduces a model of maturity in governance of ICT, including guidelines for a preliminary model and a series of good ICT governance practices that can cater to the state's deficiency, since they allow the organization's structural evolution in predefined and measurable stages.

The use of the ICT Governance Kit proposed by SEST allows identifying and evaluating the business capabilities that a state company has and its needs, considering the scope of state-owned enterprises purposes and goals, defined in a strategy and directed by the processes, artifacts and conditioning of their governance.

Increasing the efficiency of public ICT governance is one of the objectives of Brazil, according to a survey carried out by the TCU, but the ICT governance observed in Brazilian public organizations is poor [2]. Thus, improving the maturity of public ICT governance in these organizations involves the adoption of good information technology practices [3], which requires the use of modern ICT management tools and associated acquisition of goods and services [4].

Even though there is a great recognition of the importance of ICT governance and its role in organizations, the issue on how to put it in practice is still a challenge and depends on each case.

The application to public organizations makes the case even more specific and complex. Therefore, it is necessary to investigate the implementation of ICT governance in the real environment, carefully following a process to identify real problems, plan solutions, make changes and reflect on the results.

The remainder of the paper is organized as follows. Section 2 presents the background in which the theoretical bases for conducting this research are raised. Section 3 presents the list of processes adhering to state-owned enterprises and which are considered in the elaboration of the SEST Governance Kits. Section 4 defines and evaluates the maturity level of the adherent processes in the elaboration of ICT Governance Kits for State-Owned Enterprises. The conclusion of the paper is presented in Section 5 with some final remarks.

2. Background

The 1929 economic crisis produced significant losses to investors and saw the rise of very large corporations, motivating the creation of a new model for corporate control where the principal (the holder of assets or contracting party) delegates to an agent (a person hired to execute a task and that holds some execution power) the authority to decide on such assets. Given that the interests of the principal are not always aligned with those of the agent, agency conflicts may occur, i.e., the interests and motivations of the principal and the agent tend to diverge. According to [5], the agency conflict consists, in brief, of the divergence that occurs between the owners and the directors of the organization. As the directors manage the assets of others, it is considered that they cannot do so with the same degree of care and zeal as the owners of such assets. A relationship of the principal-agent can be seen in many situations such as, for example, in the relationship between officers/managers (agent) and the shareholders/owners (principal) of a corporation/organization. One of the theories developed to solve such conflicts was the agency theory formalized by [5], who also created a model for agency costs for shareholders. The costs of protecting, controlling and monitoring a business are the agency costs, defined as those required to align the interests of the agent (officers) with those of the principal (owners) [5], establishing the adoption of steps to regulate the actions of the agent. The agency theory puts forward three conditions: (i) the agent has several behaviors to resort to; (ii) the actions of the agent affect not only one's own welfare, but also that of the principal; (iii) the actions of the agent are hardly observable by the principal, as there is an information asymmetry between the parties [6].

Conflicts of interest produce costs, specifically related to monitoring the officers, which may include contracting independent audits, implementation of control measures, expenditures with insurance against losses produced by inefficient actions of the officers, compensations paid to agents linked to the increase of the wealth of the shareholders, giving shares or share options to the officers and other incentives focused on the alignment of their interests with those of the administration.

In order to reduce the conflict of interests, a system must be in place to monitor and direct the agency and reduce its costs, i.e., a system using mechanisms of governance, such as the protection of the participants to align the interests of the principal and the agent, the setting of a board of directors, the definition of a policy on officer remuneration, the publication of regular and more transparent reports, as well as structures and processes for monitoring, controlling and accounting.

Most organizations use Information and Communication Technology (ICT) as an essential business tool, and few can function without it. ICT is fundamental for managing organization resources, dealing with suppliers and customers and enabling increasingly global and dematerialized transactions. ICT is key for recording and disseminating business knowledge. In addition, It also plays a significant role in the future business plans of many organizations.

The concept of governance has replaced some traditional concepts like government, administration and management. Many scholars and institutions proposed different definitions of governance [7]. This reference defines governance as structures and processes that are designed to ensure accountability, transparency, responsiveness, rule of law, stability, equity and inclusiveness, empowerment and broad-based participation. Governance means self-organizing, inter-organizational

networks that complement markets and hierarchies as governing structures for authoritatively allocating resources and exercising control and coordination [7].

In essence, governance comprises the mechanisms of leadership, strategy and control put in place to evaluate, direct and monitor the performance of management towards the conclusion of stakeholders' goals and interests.

In this context, regarding the system whereby organizations are directed, interesting research questions arise on whether and how this system is monitored and encouraged and if it involves the best practices and relationships between the owners, board of directors, board and organ control. In the present paper, some responses to this question are proposed, considering that good corporate governance practices convert principles into objective recommendations, aligning interests with the purpose of preserving and optimizing the organization's value, facilitating access to capital and contributing to its longevity [8].

Specifically in the context of the Brazilian public administration related to state-owned companies, considering that the related governance system comprises institutional mechanisms for the development of public policies that ensure the results desired by citizens and other entities of public life, an interesting research question is if this governance system is correctly defined and achieved [9]. In the present paper, proposals for the public sector governance of ICT resources are designed to bring answers to requirements to improve the information and provision of services, encouraging the participation of society in the decision-making process and improving the levels of accountability, transparency and government effectiveness [9].

2.1. Corporate Governance

The governance system manages, monitors and stimulates the organization, involving the relationships between the owners, the board of directors, the directors and control bodies [10].

Corporate governance is the system of rules, practices and processes by which a company is directed and controlled. Currently, the governance of companies is heavily regulated by governments (in particular, public companies and stockholder companies).

Corporate governance essentially involves balancing the interests of a company's many stakeholders, such as shareholders, management, customers, suppliers, financiers, government and the community. Since corporate governance also provides the framework for attaining a company's objectives, it encompasses practically every sphere of management, from action plans and internal controls to performance measurement and corporate disclosure [11].

2.2. Public Governance

The public governance system entails the institutional mechanisms for the development of public policies that guarantee that the results expected by the citizens and other entities in the public realm are defined and attained [12]. Regulations play an important role in public governance.

Public governance is an interdisciplinary field of study centering on relationships of power between government authorities, civil society and the market, in the context of transformations in the ability of political communities to legitimately govern themselves and act effectively. These relationships can vary in nature, embodying relationships of authority (namely, authority exerted by the state, but also by the market through the enforcement of contractual arrangements), as well as the relationships of influence and persuasion, coercion and manipulation.

As such, the term not only describes changes in the nature and role of the state since the 1980s and 1990s, it also reflects the need to conceptualize a set of broad, interrelated, yet difficult to define social and political evolutions. Indeed, the popularity of governance is owed in large part to how it stands in contradistinction with a related term such as government, reflecting the attempts by scholars and practitioners to grapple with these transformations [13].

2.3. Digital Governance

Governments and citizens presently operate in a digital environment, which leaves digital trails related to whatever they do and wherever they go. These trails generate huge quantities of information about each participant, regarding each other and any interactions they have. In this context, the most important elements of an organization that deals with the citizens are the information this organization can access and the intelligence provided by the analysis of that information. Information and intelligence generate the capacity for innovation, efficiency and the agility to adapt to a rapidly changing environment [14].

Digital governance is the use by the public sector of ICT resources aimed at improving the quality of the information and the services provided, encouraging the participation of the society in the decision-making process and improving the levels of the responsibility, accountability and efficiency of the government [15].

2.4. ICT Governance

ICT governance is a key component of the overall corporate governance of the organization. It should be regarded as how ICT creates value that fits into the corporate strategy and never be seen as a discipline on its own. In taking this approach, all stakeholders would be required to participate in the decision-making process. This creates a shared acceptance of responsibility for critical systems and ensures that ICT-related decisions are made and driven by the business and not the opposite.

It is also essential that ICT governance ensures that stakeholders, business owners and other users, maintainers, operators, etc., are involved in identifying new or updated business needs and then providing the organization with the appropriate ICT (and non-ICT) solutions in order to cope with those needs.

During the development or acquisition of solutions to a particular business need, ICT governance should ensure that the selected solutions are responsive to the business and that necessary training and resources (hardware, software, tools, network capacity, etc.) are available to implement them. Monitoring activities may be carried out by internal audit or quality assurance departments, which would periodically report to management.

The ICT governance structure must be defined in order to assure that the ICT decisions, directions, resources, management and monitoring support the organization's strategies and objectives. ICT governance is a system whereby the current and future use of ICT is directed and controlled [16]. This means evaluating and targeting the use of it to support the organization and monitor its usage to accomplish the plans. It includes the strategy and its usage policies within the organization. Managers should govern state-owned enterprises through three main iterating tasks [17,18] as shown in Figure 1.

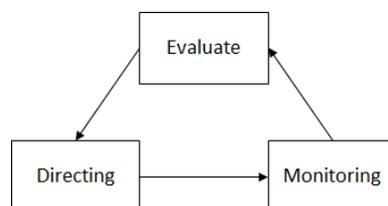


Figure 1. ICT governance tasks. Source: ISO/IEC 38500 2009 Adapted.

ICT governance is defined as how decisions and responsibilities are made and directed, to achieve a desirable behavior in the use of ICT, which refers to the alignment with the goals of the organization and coherence with its culture. In short, ICT governance consists of policies, roles, flows and rules aimed at aligning ICT with the organization's business goals, enabling it to organize and plan to obtain

the information necessary to the organization. This planning must provide mechanisms for controlling and retrieving information consistent with the needs of the organization that is incorporated [19,20].

According to the concept presented in this section, ICT governance is the system whereby the current and future use of ICT is directed and controlled, involving assessing and targeting the use of ICT to support the organization and monitoring its use to carry out plans, including ICT use strategy and policies inside an organization [17].

Management is responsible for the planning, implementation, monitoring and development of ICT activities in line with the direction defined by the governance function to attain corporate goals [21,22].

2.5. High Management

High management consists of public authorities responsible for ICT governance in the bodies and entities of the Brazilian Public Administration, i.e., the State Secretaries, who hold positions of a special nature or are in position of cabinet-appointed commissions as Senior Directors and Advisors (in Portuguese, *Direção e Assessoramento Superior—DAS*) of Level 6 or equivalent [23]. It is worth to point out that high management has the responsibility to govern ICT, i.e., to guarantee that the ICT is working in an integrated manner, adding value to the business[23].

2.6. Difference between ICT Governance and ICT Management

ICT governance is the system through which the present and future use of ICT is directed and controlled, involving the assessment and directing of ICT to support the organization, as well as the monitoring of its use to implement plans, including the ICT strategy and policies within an organization [17].

By contrast, management is responsible for the planning, development, execution and monitoring of ICT activities, in line with the guidance set by the governance area, to attain the corporate goals [21]. Figure 2 shows the basic functions, as well as the roles that are responsible for both ICT management and governance.

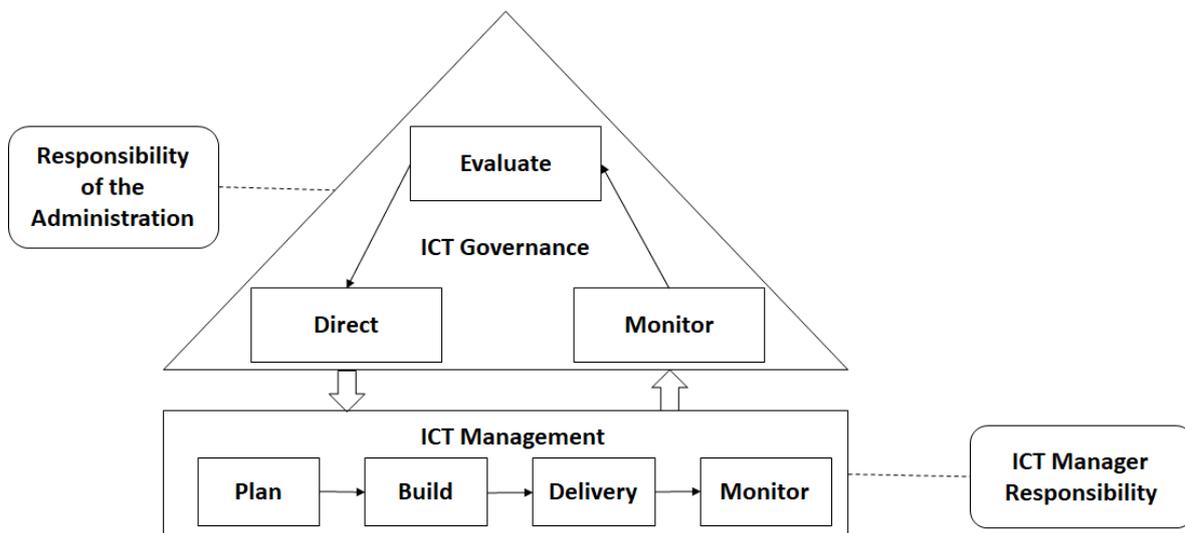


Figure 2. ICT management tasks and their relation to ICT governance. Source: ISO/IEC 38500 2009 Adapted.

3. Processes Considered in the Design of SEST Governance Kits for State-Owned Companies

Organizational structures are a key element of ICT governance in articulating the roles of the various management and governance bodies across the business and decision-making process.

They should assign clearly-defined delegation of duties regarding decision-making and performance evaluation and monitoring.

Organizational structures must also be supported by appropriate standards, policies and procedures, which should enhance the organization decision-making capacity. Organizational structures are influenced by the stakeholders, i.e., all groups, organizations, members or systems that affect or can be affected by an organization actions. Examples of important external stakeholders for public organizations include the Parliament, state-owned enterprises, the Congress, other government entities and the citizens.

Organizational structures are also influenced by the users, both internal and external. Internal users are the business executives, functional departments that own business processes and individuals within the organization who interact with business processes. External users are the agencies, individuals and others who use the products or services provided by the organization (for example, other departments, citizens, public companies). Another influence on organizational structures is comprised of the providers, for example companies, units or persons, both internal and external, that provide services to the organization.

Methodology

The processes that are appropriate for state-owned enterprises and that are considered in the elaboration of SEST ICT Governance Kits have been identified from the cross-examination of the basic governance reference recommendations from: (a) the TCU (ICT governance (TCU)) [9], (b) the Control Objectives for Information and Related Technologies (COBIT) [21] and c) the Management System for Information Technology Resources (in Portuguese, Sistema de Administração dos Recursos de Tecnologia da Informação—SISP) which is coordinated by the Brazilian Ministry of Planning, Development and Management [24].

The ICT governance model proposed for the SISP has principles and guidelines that should be observed by the bodies and entities of the system during the implementation of their ICT governance. Beyond that, the model is built on the concepts of conditioning practices. The model has ten practices, the accomplishment of which is important in the improvement of ICT governance in the organization. For each one of the practices, it presents the related conditioning factors that influence the execution of that practice, favorably or otherwise. In all, sixty-three (63) conditioning factors were identified. The model also shows the relation that exists between the practices, grouping them according to the tasks of ICT governance—evaluation, direction and monitoring—and the relation between the tasks of ICT management and governance.

Table 1 lists the most appropriate processes (18 processes) to state and that are considered in the elaboration of the SEST Governance Kits. The definition and the choice of processes presented in Table 1 to compose the SEST ICT Governance Kit were carried out by an ICT committee, which was composed of five specialists in ICT governance and three representatives from SEST, also involved in ICT governance. All the authors of this work were part of the analysis of the processes existing in the governmental guides (ICT governance-(TCU and SISP)) and in COBIT. The 18 processes are considered as adhering to the needs of SEST.

Table 1. State of the government processes for the elaboration of Governance Kits.

Number	Adherent Processes
1	ICT Committee.
2	ICT Risks Management.
3	ICT Projects and Services Portfolio.
4	Hiring of ICT Goods and Services (Managing Software Acquisitions)
5	Management of ICT People (Empowerment, Performance, Roles and Responsibilities).
6	Information Technology Director Plan (ITDP).
7	ICT Security Committee.
8	Business Process Modeling (Automated Automating).
9	Catalog of Computerized Systems (ICT Services Catalog).
10	ICT Services Continuity Management.
11	Process of Managing Changes.
12	Incidents and Problems Management Process (Service Center).
13	Information and Communication Security Policy.
14	Information Security Risk Management.
15	Software Development Process (Quality Management, Configuration).
16	ICT Projects' Management.
17	ICT Contracts' Management Process.
18	Manage ICT Assets (Hardware, Licenses and Costs).

4. Processes of the State in the Elaboration of Kits 1, 2 and 3 of SEST Governance

This section defines and evaluates the maturity level of the adherent processes in the elaboration of ICT Governance Kits for state-owned enterprises. This evaluation was conducted based on the definition of COBIT to maximize the combined effects of COBIT 5 [21] and the Capability Maturity Model Integration (CMMI): A guide to using the tool practices pathways [25].

COBIT 5 has a set of guidelines and best practices for the governance and management of different areas of ICT (such as security, risks, etc.) [26]. This tool is designed to assist COBIT users with CMMI [27]. The tool highlights areas of COBIT that can leverage CMMI maturity practices.

CMMI is a reference model that contains the necessary practices for maturity, being used by organizations that want to operate with high performance. For this, based on the organization's business goals, CMMI provides a set of practices for process improvement [28]. As the organization's processes are created or changed, they must be mapped to the process areas so that their progress can be evaluated according to the CMMI model. This evaluation is done through levels, describing an evolutionary or evaluative path to improve the performance of the institution's processes. They can be applied to process groups within the institution or the institution as a whole.

The improvement paths in CMMI follow a set of maturity levels, which are used to characterize organizational improvement relative to a set of process areas and corresponding to a representation by stages and capacity levels, which characterize organizational improvement on a single process area and utilize continuous representation. To achieve a level, the organization must fulfill a series of objectives of an area or a set of process areas [28]. The CMMI maturity levels are:

- **Maturity Level Number 1: maturity level: initial.** Description: At this level, the processes are usually chaotic and ad hoc, and the organization does not provide a stable environment to support the processes. Therefore, success in these cases often depends on the competence and effort of the people involved, not on the proven effectiveness of the processes. What often also happens is that sometimes, the products and services succeed, but they exceed the budget and schedule documented in the planning.
At Level 1, organizations have the usual tendency to commit themselves, abandon their processes when a crisis occurs and thus are unable to repeat the successes previously achieved.
- **Maturity Level Number 2: maturity level: managed.** Description: When we reach this level of maturity, the organization already has enough discipline to ensure that existing practices can be

ensured even in times of crisis. When these practices are effective, the processes are executed and managed according to their documented designs; for example, monitoring the status of products at certain defined points in their cycle and establishing commitments among important stakeholders of the product.

All this results in projects that ensure processes that are planned and executed according to a policy, qualified personnel, adequate resources, that produce controlled outputs and in a monitored, controlled, reviewed and evaluated way to adhere to the process description.

- Maturity Level Number 3: Maturity level: Defined. Description: At this level, processes reach a much larger stage of characterization and understanding, are described in patterns, procedures, and establish consistency for the organization. The biggest difference between levels of maturity 2 and 3 is the scope of patterns, description of processes and procedures, because on level 3, to meet a project, there should be an adaptation from the standard process set of the organization and not different versions of patterns for each project.

The consolidated default processes are more proactively managed by making talking about interrelationships between process activities and improved over time and require a more stringent description of you compared to level 2. A duly defined process declares: purpose, entries, input criteria, activities, roles, metrics, verification steps, output, and output criteria.

- Maturity Level Number 4: maturity level: quantitatively managed. Description: To reach this level, the organization through its projects must establish quantitative objectives to obtain quality and performance in the processes. A major difference between Levels 3 and 4 is the predictability that is made through quantitative and statistical analysis of process data when it comes to Level 4.

The quantitative goals to be achieved consider the needs of the organization's customers, users and process implementers. When a sub-process is selected, specific performance measures are collected and statistically analyzed. In this case, it is important to see the relationship between the different processes and their impact on the achievement of the objectives of the process, to apply the quantitative and statistical techniques where the organization is most valuable.

- Maturity Level Number 5: maturity level: in optimization. Description: At Level 5, the organization focuses on improving process performance through incremental, innovative process and technology improvements based on a quantitative understanding of its business objectives and performance needs.

These objectives must be established, continually revised to reflect changes in organizational performance, measured and compared to quality objectives and used as criteria in process improvement management. If data analysis identifies performance failures, they are used to drive organizational process improvement.

One aspect that differentiates levels is that in Level 5 the focus is on the management and improvement of the organizational performance using data collected from multiple processes, while in Level 4, the organization and its projects are focused on understanding and controlling performance at the sub-process level, using the results to manage projects.

The COBIT 5/CMMI Practices Pathways Tool provides connections between COBIT and CMMI to identify and highlight their related components; assisting in designing or improving governance structures. The most relevant connection points between COBIT and CMMI models are their practices. The analysis of the models was conducted with the objective of establishing not only the alignment between the two, but also among their practices, mapping the relationships between the practices of both models.

However, CMMI and COBIT were designed for different purposes, so they do not align perfectly. Therefore, there are cases where connections between them do not make sense. In such cases, the Practices Pathways Tool shows that there is no way to align practices between models. It is also possible that a practice in a model aligns with multiple practices in the other, and when this occurs, the tool also shows the user the multiple alignments. The tool was designed to allow guidance on

a model based on the other. That is, from CMMI, it can be guided in COBIT practices, or COBIT in CMMI practices.

The COBIT 5/CMMI Practices Pathway Tool was built as a Microsoft Excel worksheet. The tool consists of a worksheet that relates CMMI and COBIT practices. Specific elements of each practice are in separate columns to provide the user with the opportunity to classify and filter the data according to their needs.

To specify a practice element to be examined, the user must click on the filter icon and select the element value in the list of displayed values, and the tool will be updated to show the results of the selected filter. The use of this tool allows businesses to look beyond the management of information technology resources, traditional use of COBIT, software development and traditional CMMI use, considering broader implications of practices and their connections to the value delivery for stakeholders [25].

Table 2 shows all the processes of the State Governance Kits.

Table 2. Processes of the State Governance Kits.

Number	Adherent Processes	Maturity Level	Artifacts	Estimated Deadline for Deployment
1	ICT Committee.	2	Internal Standard of Creation of the ICT Committee. Internal Rules of the ICT Committee. Meeting Minutes of the ICT committee.	1 month.
2	ICT Risks Management.	3	ICT Risk Management Plan. ICT Risk Management Policy. Information and Communication Security Policy.	12 months.
3	ICT Projects and Services Portfolio.	2	ICT Projects and Services Prioritization Criteria. Prioritization Policy. Project Portfolio and ICT Services from State.	3 months.
4	Hiring of ICT Goods and Services (Managing Software Acquisitions)	3	Official Demand Document. Hiring Planning Team. Compromise Term Model. Model of the Term of Science. Reference Term or Basic Design.	6 months.
5	Management of ICT people (Empowerment, Performance, Roles and Responsibilities).	2 and 4	Talent Bank (Skills and Competences). Form the Definition of Roles and Responsibilities. Metrics to Evaluate Performance. Training Plan.	3 months to Level 2. 12 months to Level 4.
6	Information Technology Director Plan (ITDP).	2	Internal Standard for the Designation of the ITDP Team. Standard of Guide The ITDP. ITDP Monitoring Report Model. Model List of Principles and Guidelines. SWOT Analysis Model. Needs Inventory Model. Model of Goals and Action Plan. Budget Plan Model. Model of Risk Management Plan. Model of Management Plan for People. ITDP Timeline Model. Model of Work Plan for the Elaboration of the ITDP.	6 months.
7	ICT Security Committee.	4	Internal Standard of Creation of the ICT Security Committee. Internal Rules of the ICT Security Committee. Meeting Minutes of the ICT Security Committee.	1 month.
8	Business Process Modeling (Automated/Automating).	3	Form the Definition of Roles, Responsibilities, Access Privileges and Authority Levels. Simplifying Business Process Modeling Document.	12 months.
9	Catalog of Computerized Systems (ICT Services Catalog).	2 and 3	Form with the ICT Managers and the Business Areas. ICT Services Catalog. Service Level Agreement. Metrics and Indicators for Performance of Services and Service Level Agreements.	3 Months to Level 2 6 Months to Level 3.
10	ICT Services Continuity Management.	4	Service Continuity Plan. Service Continuity Policy.	12 Months.
11	Process of Managing Changes.	3 and 5	Change Management Plan. Configuration Management Plan. Change Report. Causal Analysis Report.	6 months to Level 3. 12 months to level 5.
12	Incidents and Problems Management Process (Service Center).	3	Incident Management Plan. Knowledge Base. Incident Report and Status. Report on Service Requisitions and Incidents. Problem Management Plan. Corrective Action Report.	12 months.

Table 2. Cont.

Number	Adherent Processes	Maturity Level	Artifacts	Estimated Deadline for Deployment
13	Information and Communication Security Policy.	4	Form the Definition of Roles and Access Privileges. Information Classification Form. Information and Communication Security Policy.	12 months.
14	Information Security Risk Management.	3	Form the Categories and Parameters for the Risks of Information Security. Information Security Risk Management Plan. Risk Treatment Plan of Information Security.	9 months.
15	Software Development Process (Quality Management, Configuration).	2 and 3	Software Development Process. Quality Management Plan. Test Plan. Requirements Traceability. Solution Maintenance Plan. Audit Plan and Baselines. Quality Measurement Metrics Report. Report Measuring Metrics of the Configuration. Measurement Document. Reports of Quality Standards, Practices and Procedures. Improvement Plan.	2 months to Level 2. 12 months to Level 3.
16	ICT Project Management.	4	Report of the Identified Projects. Project Prioritization Criteria. Prioritized Projects Report. Project Integration Management Plan. Project Scope Management Plan. Project Time Management Plan. Project Cost Management Plan. Project Quality Management Plan. Project Human Resources Management Plan. Project Communications Management Plan. Project Risk Management Plan. Project Acquisition Management Plan. Project Stakeholder Management Plan. Project Management Plan. Project Performance Report.	6 months.
17	ICT Contracts' Management Process.	3 and 4	Edict. Reference Term or Basic Project. Indicators and Metrics to Gauge the Results. Service Orders or Goods Supply. ICT Contract Management Plan. Communications to the Contract. Provisional Receiving Term. Final Receiving Term. Rejection Term. Vendor/Contracted Performance Report. (Level 4) Product Validation Criteria and Methods. Product and Component Validation Report.	12 months to Level 3. 6 months to Level 4.
18	Manage ICT Assets (Hardware, Licenses and Costs).	3	ICT Assets' Report. Software Licenses' Report. License Management Plan. Indicators and Metrics to Manage Hardware Asset Capacity and Performance. Hardware Asset Performance Report.	12 months.

Figure 3 presents the list of processes that will compose the Processes of Kit 1, with their respective artifacts and their level of maturity.

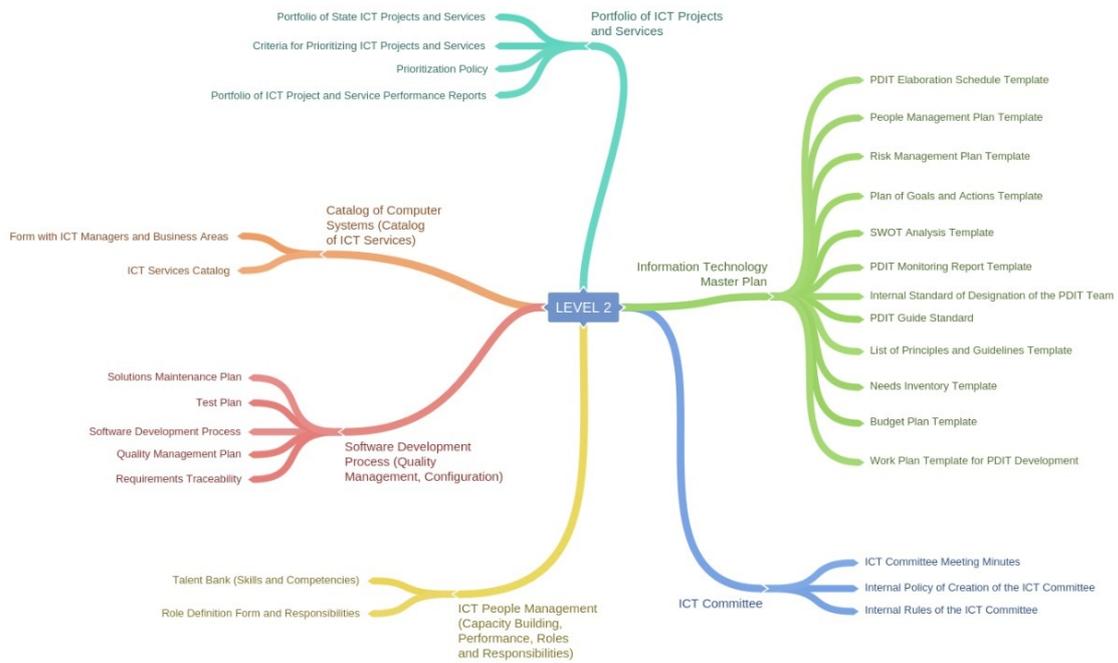


Figure 3. Processes of Kit 1.

Figure 4 presents the list of processes that will compose the Processes of Kit 2, with their respective artifacts and their level of maturity.

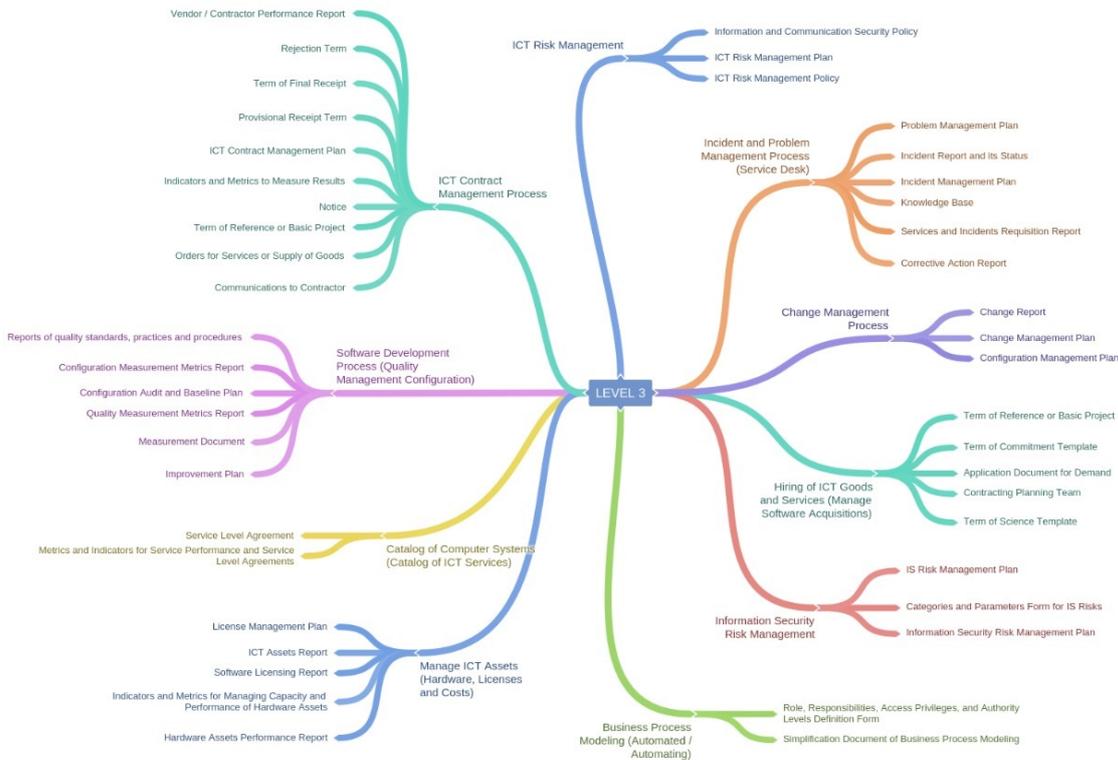


Figure 4. Processes of Kit 2.

Figure 5 and 6 presents the list of processes that will compose the Processes of Kit 3, with their respective artifacts and their level of maturity.

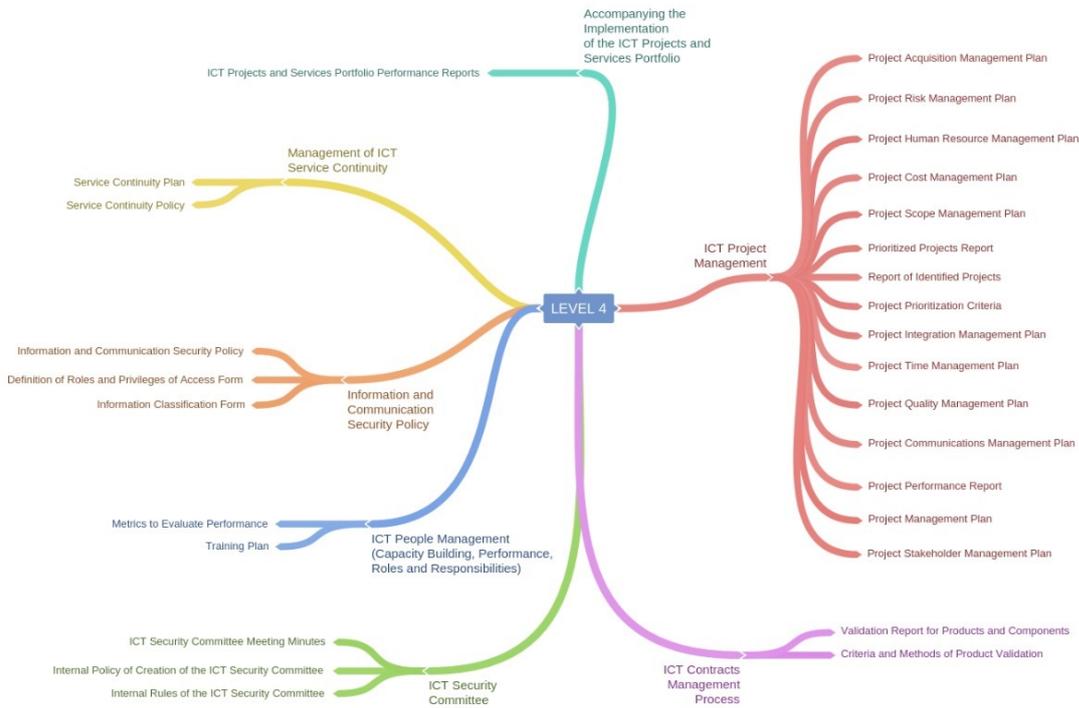


Figure 5. Processes of Kit 3, Level 4.

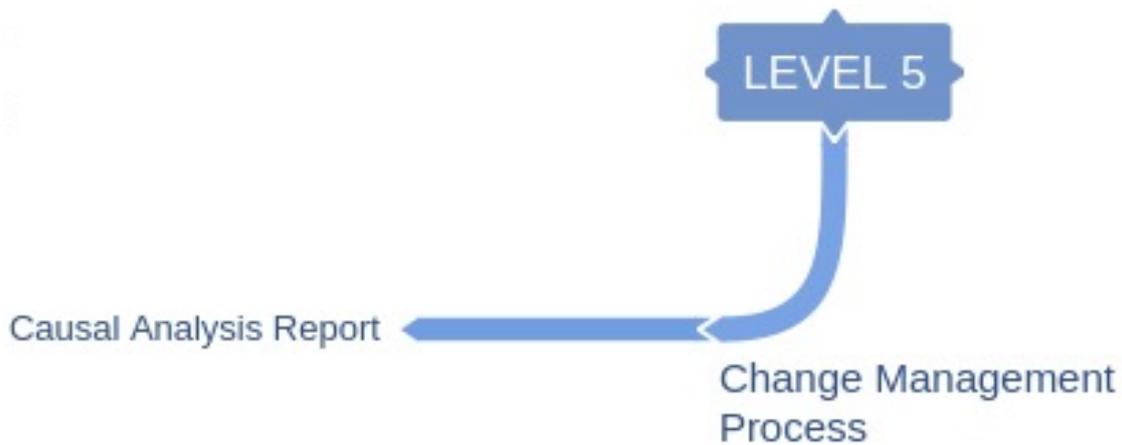


Figure 6. Processes of Kit 3, Level 5.

4.1. Continuous Improvement Approach

This Kit offers a generic continuous improvement approach, based on the Deming cycle (Plan, Do, Check, Act (PDCA)) and on the life cycle of implementation, as proposed by the COBIT 5 [21].

With this approach and having the ICT governance presented in this Kit as a background, the intention is that the bodies and entities in the SEST, independently of the level of maturity of their management practices and ICT governance, can streamline, in a continuous way, their ICT governance systems. Figure 7 shows the six stages that form the generic approach on continuous improvement put forward in the ICT Governance Kit.

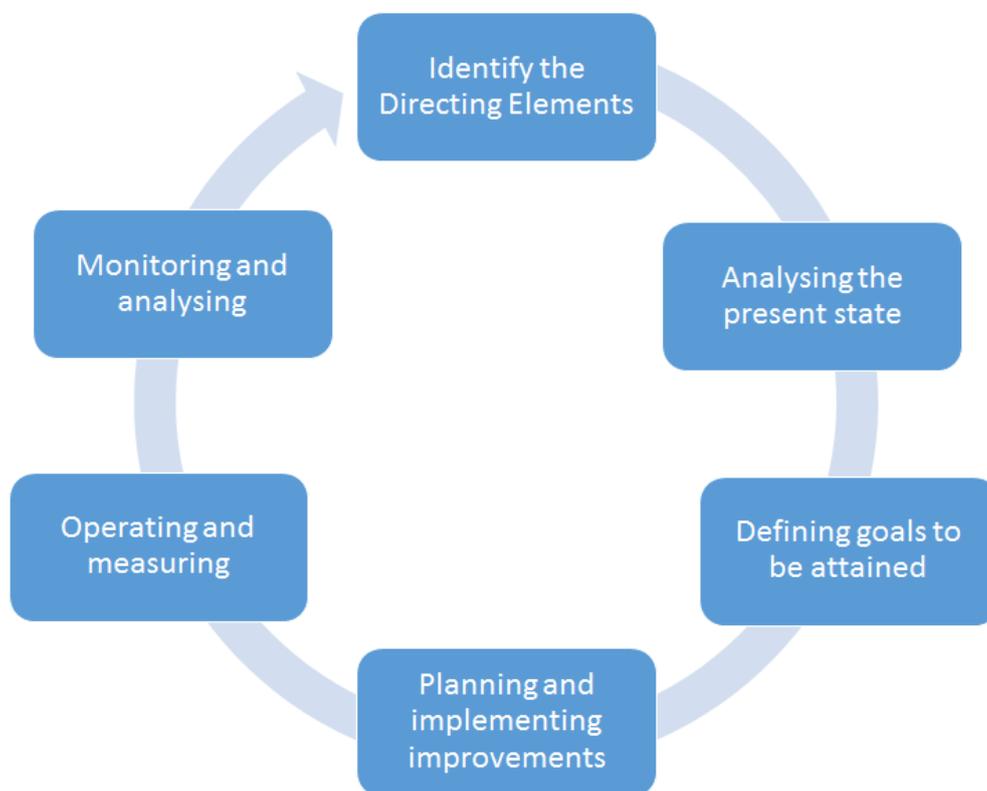


Figure 7. Continuous improvement approach [21], adapted.

Detailed Description of the Continuous Improvement Approach

It is recommended that the work of continuous improvement of the ICT governance within an organization should be done and monitored by a program. A program is defined as a group of related projects, managed in a coordinated manner, to obtain the benefits and control that would not otherwise be at hand, if they were managed individually [9]. The stages shown in Figure 7 are as follows.

Stage for identifying the directing elements: In this stage, the organization should identify the directing elements that will influence the configuration of the arrangements that form the ICT Governance Kit, such as:

- Institutional mission and vision;
- Strategic references of the government, as issued by the SISP, TCU, COBIT, and of the organization, such as the ICT Director Plan (in Portuguese, Plano Diretor de Tecnologia da Informação e das Comunicações—PDTIC) and the Strategic Information Plan (in Portuguese, Plano Estratégico da Informação—PEI), for example;
- Legislation applicable to the organization, as listed by [29];
- Needs of the parties interested in the use of ICT.

Stage for the analysis of the present state: In this stage, the organization should study the present state of the arrangements that form its ICT Governance Kit, including its policies, processes, organizational structures or equivalent functions.

Stage for defining the goals to be achieved: Based on the identification of the directing elements, and taking into account the present state of the arrangements that form its ICT Governance Kit, the organization should define, in a clear and non-ambiguous manner, the goals for improvement to be reached by its ICT Governance Kit.

Stage for planning and implementing the improvements: Based on the goals defined in the previous stage, the organization should plan and implement the improvement actions needed for its ICT Governance Kit to attain the results expected.

Stage for operating and measuring: In this stage, the organization should measure, continuously, the operation of the arrangements made in its ICT Governance Kit, aiming at collecting information for its analysis and monitoring.

Stage for monitoring and analyzing: In this stage, the organization should monitor and verify based on the data collected in the previous stage; whether the implementing of the improvement actions in the arrangements that form its ICT Governance Kit have obtained the expected results (based on the goals set at first). The identification of deviations in this activity should produce a set of actions to correct the work to implement improvements in the ICT Governance Kit of the organization, providing continuous improvement, in a new cycle.

During the process of preparation and implementation of its ICT Governance Kit, the organization should take into consideration its institutional missions, the public services provided to society, the needs of the parties interested, as well as the present level of maturity of its management practices and ICT governance. The analysis of the organizational domain, through the lenses of these elements, will help the organization to define the features of its ICT Governance Kit, which will be different from one organization to another.

Given the diversity of the organizations governed by SEST, in terms of the maturity of their management practices and ICT governance, this paper proposes a sequence for the implementation of the ICT Governance Kit, taking into consideration the inter-dependencies that exist amongst them, both in the maturity level, as well as in the level of adherent processes and artifacts.

5. Conclusions

This work presents a survey of ICT governance best practices and conditioning that are considered relevant to execute a diagnosis of practices to be adopted by the Brazilian government Secretariat of Coordination and Governance of State-Owned Enterprises Secretary (SEST).

To conduct an effective ICT governance cross-examination, all practices present in governance evaluation techniques for information and communication technology of the Brazilian Federal Court of Accounts (TCU (ICT governance)), the SISP and the COBIT 5.0 were used to identify which processes were considered important for state-owned enterprises governed by SEST. With the processes, conditioning and artifacts identified, the SEST Information and Communication Technology Governance Kits were proposed.

According to the Capability Maturity Model Integration (CMMI), the Kits were divided into Kit 1 (with its processes considered as Maturity Level 2), Kit 2 (with its processes considered as Maturity level 3) and Kit 3 (with its processes considered as Maturity Levels 4 and 5). It is hoped that with the use of these ICT Governance Kits, Brazilian state-owned enterprises would improve their level of maturity and have a better evaluation by the main government auditing agency, the TCU.

As future work, we plan study cases to apply these ICT Governance Kit proposals to selected state-owned enterprises and to check their maturity levels regarding ICT governance practices. The deployment and the performance of the adoption process for these ICT Governance Kits will be monitored so as to have state-owned enterprises governed by SEST in compliance with ICT governance recommendations from TCU.

Author Contributions: The conceptualization of the ICT Governance Kits was made by E.D.C and G.D.A.N. while their linking to maturity levels was made by R.T.d.S.J. and R.P.d.C. All authors contributed to Writing—Original Draft Preparation and Writing—Review & Editing.

Acknowledgments: This research work has the support of the Brazilian Ministry of Planning, Development and Management (Grants 11/2016 SEST—Secretariat of Coordination and Governance of State Enterprises, and 005/2016 DIPLA—Directorate of Planning and Management), as well as the Support Center for Technological Development (CDT) of the University of Brasília (UnB).

Conflicts of Interest: The authors declare no conflict of interest.

References

- De Haes, S.; Van Grembergen, W. Enterprise governance of information technology. In *Achieving Alignment and Value, Featuring COBIT*; Springer: Berlin/Heidelberg, Germany, 2015; Volume 5.
- Sales, L.M.G.M. Percepção de Gestores de TIC da APF Sobre Boas Práticas de Governança de TIC. Monograph (Bachelor of Information Systems)—Department of Computer Science, Center of Exact Sciences and Technology, Federal University of Sergipe 2017. Available online: <http://ri.ufs.br/jspui/handle/riufs/7032> (accessed on 7 June 2018).
- Solar, M.; Murua, S.; Godoy, P.; Yañez, P. Correlation Between ICT Investment and Technological Maturity in Public Agencies. In Proceedings of the International Conference on Electronic Government, St. Petersburg, Russia, 4–7 September 2017; Springer: Berlin/Heidelberg, Germany, 2017; pp. 411–420.
- França, A.; Figueiredo, R.; Venson, E.; Silva, W. Storytelling on the implementation of a Decentralized Model for Software Development in a Brazilian Government Body. In Proceedings of the 17th International Digital Government Research Conference on Digital Government Research, Shanghai, China, 8–10 June 2016; ACM: New York, NY, USA, 2016; pp. 388–396.
- Jensen, M.C.; Meckling, W.H. Theory of the firm: Managerial behavior, agency costs, and ownership structure. In *Economics Social Institutions*; Springer: Berlin/Heidelberg, Germany, 1979; pp. 163–231.
- Dominici, G.; Yolles, M. Decoding the XXI Century's Marketing Shift: An Agency Theory Framework. *Systems* **2016**, *4*, 35. [[CrossRef](#)]
- Xia, S. E-Governance and Political Modernization: An Empirical Study Based on Asia from 2003 to 2014. *Adm. Sci.* **2017**, *7*, 25. [[CrossRef](#)]
- Instituto Brasileiro de Governança Corporativa. Código das Melhores Práticas de Governança Corporativa; IBGC: São Paulo, Brazil, 2009. Available online: http://www.ibgc.org.br/userfiles/Codigo_julho_2010_a4.pdf (accessed on 7 June 2018).
- Tribunal de Contas da União. Referencial Básico de Governança Aplicável a Órgãos e Entidades da Administração Pública. TCU: Brasília, Brazil, 2014. Available online: <http://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A14DDA8CE1014DDFC35CA83C74> (accessed on 7 June 2018).
- Matias-Pereira, J. A governança corporativa aplicada no setor público brasileiro. *Adm. Pública Gest. Soc.* **2010**, *2*, 109–134.
- Tricker, R.B.; Tricker, R.I. *Corporate Governance: Principles, Policies, and Practices*; Oxford University Press: Oxford, MS, USA, 2015.
- Osborne, S.P. *The New Public Governance: Emerging Perspectives on the Theory and Practice of Public Governance*; Routledge: Abington, UK, 2010.
- Grossi, G.; Papenfuß, U.; Tremblay, M.S. Corporate governance and accountability of state-owned enterprises: relevance for science and society and interdisciplinary research perspectives. *Int. J. Public Sect. Manag.* **2015**, *28*, 274–285. [[CrossRef](#)]
- Dunleavy, P.; Margetts, H. Design principles for essentially digital governance. In Proceedings of the 111th Annual Meeting of the American Political Science Association, San Francisco, CA, USA, 3–6 September 2015.
- Dahlbom, B. The Digital Revolution. *Proceedings* **2017**, *1*, 163. [[CrossRef](#)]
- Silva, M.B.D.D.; Silva, E.C.; Filho, F.A.D.C.; Garcia, T.M.; Nunes, I.; do Nascimento, R.P.C. Public ICT Governance: A Quasi-systematic Review. In Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), Porto, Portugal, 26–29 April 2017; Volume 2, pp. 351–359.
- Calder, A. *ISO/IEC 38500: The IT Governance Standard*; IT Governance Ltd.: Ely, UK, 2008.
- Taft, T.H. The Integration of IT Governance, Information Security Leadership and Strategic Alignment in Healthcare: A Correlational Study. Ph.D. Thesis, Capella University, Minneapolis, MN, USA, 2017.

19. Weill, P.; Ross, J.W. *IT Governance: How Top Performers Manage IT Decision Rights for Superior Results*; Harvard Business Press: Brighton, MA, USA, 2004.
20. Kien, S.S.; Soh, C.; Weill, P. IT Governance in Global Enterprises: Managing in Asia. In Proceedings of the International Conference on Information Systems (ICIS 2008), Paris, France, 14–17 December 2008; p. 97.
21. ISACA. *COBIT 5: A Business Framework for the Governance and Management of Enterprise IT*; ISACA: Rolling Meadows, IL, USA, 2012.
22. Clara, A.M.C.; Canedo, E.D.; de Sousa Júnior, R.T. Elements that Orient the Regulatory Compliance Verification Audits on ICT Governance. In Proceedings of the 18th Annual International Conference on Digital Government Research, Staten Island, NY, USA, 7–9 June 2017; ACM: New York, NY, USA, 2017; pp. 177–184.
23. De Mendonça, C.M.C.; Guerra, L.C.B.; de Souza Neto, M.V.; de Araújo, A.G. Governança de tecnologia da informação: Um estudo do processo decisório em organizações públicas e privadas. *Rev. Adm. Pública* **2013**, *47*, 443–468. [[CrossRef](#)]
24. Ministério do Planejamento, Orçamento e Gestão. *Estratégia de Governança Digital da Administração Pública Federal*. MP: Brasília, Brazil, 2016. Available online: <https://www.governodigital.gov.br/documentos-e-arquivos/egd-estrategia-de-governanca-digital-da-administracao-federal-2016-2019.pdf> (accessed on 7 June 2018).
25. ISACA and CMMI Institute. *Maximizing the Combined Effects of COBIT 5 and CMMI: A Guide to Using the Practices Pathways Tool*. ISACA: Rolling Meadows, IL, USA, 2017. Available online: <http://www.isaca.org/COBIT-CMMI-Connections> (accessed on 7 June 2018).
26. Patón-Romero, J.D.; Baldassarre, M.T.; Piattini, M.; García Rodríguez de Guzmán, I. A Governance and Management Framework for Green IT. *Sustainability* **2017**, *9*, 1761. [[CrossRef](#)]
27. CMMI Product Team. *CMMI for Development, Version 1.3*. Technical Report CMU/SEI-2010-TR-033, CMU/SEI: Hanscom AFB, MA, USA, 2010. Available online: https://resources.sei.cmu.edu/asset_files/TechnicalReport/2010_005_001_15287.pdf (accessed on 7 June 2018).
28. Chaudhary, M.; Chopra, A. CMMI Overview. In *CMMI for Development*; Springer: Berlin/Heidelberg, Germany, 2017; pp. 1–7.
29. Cardoso, A.G. Governança Corporativa, transparência e compliance nas empresas estatais: O regime instituído pela Lei 13.303/2016. *Estatuto Juríd. Empresas Estatais Lei* **2016**, *13*, 94–119.



© 2018 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0/>).