International Journal of Computer Information Systems and Industrial Management Applications.
ISSN 2150-7988 Volume6 (2014) pp. 505-514

Governance of Service-Oriented Architecture through the CommonGov Approach

Haroldo Maria Teixeira Filho[1,2] and Leonardo Guerreiro Azevedo[2]

[1] Information and Services Administration, Petróleo Brasileiro S/A
General Canabarro, 500 – 4th Floor, Rio de Janeiro, Brazil
haroldo.filho@uniriotec.br

[2] Graduate Program in Informatics, Federal University of State of Rio de Janeiro,
Av. Pasteur, 458, Rio de Janeiro, Brazil
azevedo@uniriotec.br

***Abstract*: Service-Oriented Architecture (SOA) is a paradigm used by organizations to reduce costs and foster agility through reuse of assets and an increase of alignment between business and IT. To achieve these benefits, a governance model is vital to ensure that technical actions and decisions of IT departments are aligned to organizations' business goals and requirements. There are several proposals of SOA governance models in academia and industry. However, there are important differences between them concerning process, elements and definitions they propose. This work analyzes the main current SOA governance models proposed by literature, and presents a consolidate approach aiming to create a governance model that addresses the most important issues for organizations.**

***Keywords*:** SOA, Governance, Services**.**

I. Introduction

SOA (Service-Oriented Architecture) is a strategy to reorganize an initially isolated portfolio of applications into an interconnected set of services, accessible by standard interfaces and communication protocols. The construction of applications is largely simplified through the composition of existing services [1].

SOA promotes several gains to organizations as highlighted by [1], [2], [3]. Among these advantages, we emphasize lower development and maintenance costs, shorter delivery times and greater flexibility and stability of solutions.

However, the Open Group [4] presents that companies that have approached SOA through a pilot project did not reach the same benefits when adopting the approach in the whole organization. When the approach goes from one division (considered in the pilot project) to multiple ones new challenges rise, making difficult to accomplish the aimed benefits. Schepers et al. [5] and Niemann et al. [3] present the following main challenges:

- Ensure compliance with internal, technical and legal regulations;
- Address new roles and responsibilities, due to new stakeholders in the SOA context;
- Promote a culture of sharing and reuse of assets instead of constant application development;
- Define a financial model that enables service sharing;
- Control the impact of changes in an environment where dependencies are established between several stakeholders.

Service governance is pointed by several authors [3], [6], [7] as the best approach to meet such requirements. Janiesch et al. [7] defines SOA Governance as the establishment of structures, processes, policies and metrics appropriate to ensure the adoption, implementation, operation and evolution of a Service-Oriented Architecture aligned with business objectives and compliant with laws, regulations and best practices.

The academy [3], [6], [7], technology vendors [8], [9], [10], [11] and consortiums [4] have already proposed models for SOA Governance. However, these approaches address distinct aspects, and are described in different level of detail. There is a lack of consensus about the required elements for composing a governance model.

Niemann et al. [12] presents that the current models do not address all the required activities for service lifecycle and there is a lack of steps to regulate service consumption between different organizations. Janiesch et al. [13] also support the last concern, and emphasizes that current approaches do not deal with cross-organizational scenarios since they do not carry out activities for dealing with billing and monitoring in this context. Besides, there is a lack of legal and security mechanisms to ensure compliance and a safe architecture. In other work, Janiesch et al. [7] point to low coherence between the concepts' definitions considered by the governance models.

Due to this reasons, a consolidated approach for SOA Governance is required, whose aim is to simplify and reduce the risk of the establishment of SOA in organizations.

The goal of this work is to identify the required processes to establish a governance model for SOA based on the academia and industry proposals in order to establish an integrated

approach. Besides, it highlights the gaps and similarities between existing models. Besides, this work corresponds to the preliminary work presented by Teixeira Filho and Azevedo[14].

This work is divided as follow. The first section is the current introduction. Section 2 presents the related work. Section 3 presents our proposal for SOA governance, while Section 4 compares this proposal with the related works. Finally, Section 5 presents the conclusion and future work.

II. Related Work

Niemann et al. [3] define a structure for SOA Governance Models, and derived the following basic concepts to structure a model:

- Establishment of a central structure to steer the SOA initiatives, along with the definition of new roles and accountabilities;
- Definition of a best practices catalog and a set of governance policies;
- Formalization of service lifecycle, i.e., to assume a service development cycle;
- Formalization of SOA roadmaps to define the milestones to check the overall evolution of the architecture;
- Definition of metrics to assess achievements, benefits and evolution of the SOA initiatives;
- Establishment of controls for operational processes;
- Definition of policy enforcement mechanisms to ensure compliance with goals and directives;
- Use of a SOA maturity model for benchmark comparison and planning capabilities needed for running SOA.

Based on these elements, the authors proposed a governance model composed by five components: organizational governance entities, governance policies, best practices catalog, compliance observation and SOA maturity measurement. The drawback in this work is that Niemann et al. defines each of these items, but does not presents what are the processes for SOA governance. So, their model was employed in our work to organize concepts and derive the main groups of processes for SOA governance.

Janiesch et al. [13] define a model based on CObIT[15] and ITIL[16]. They evaluated the processes proposed in these two models and related their application to a SOA context. They made explicit which processes should be extended and which ones are missing. Their analysis resulted in five stages representing the service lifecycle (design, deployment, delivery, monitoring and change). However, the authors do not present the definition of the proposed processes. They only classify process into stages and point if each one is partially or fully presented in CObIT or ITIL. Another important aspect of this work is the necessity to improve governance models to enable SOA solutions on the Internet in order to develop service compositions available from multiple organizations. This scenario consists in an Internet of Services and it yields new challenges, mainly security concerns.

The model proposed by the Open Group [4] divides the governance processes in two categories: governance processes (to regulate the model), and governed processes (to deal with the operation of the architecture). The governed processes are divided into four sets – service portfolio management, service lifecycle management, solution portfolio management and solution lifecycle management, including the necessity to apply governance not only for services, but also for the applications composed with the services. However, this model deals with technical and strategy issues, but lacks specific processes to handle cultural change and security monitoring.

Hojaji and Shirazi [6] define another model based on CObIT, considering four domains for governance processes – plan, define, implement and measure. These elements control processes to effectively deploy and manage services, divided into strategy, design, transition and operation domains. However this model does not consider all the aspects of service consumers. It do not present specific processes to deal with service composition and composite solution management

Bennet [8] (Oracle proposal) proposes a model based on the Open Group work, considering similar processes, but combining service and solution portfolio management in one domain named as SOA portfolio management. Besides, Bennet [8] extended the control processes to include tasks to enforce organizational change management, including specific activities for communication, training and evangelism, aiming to act over the organizational culture. These steps were considered in our approach. On the other hand, some processes are missing in their approach, such as: conformity, service identification and infrastructure monitoring.

The Butler/Gartner group [11] proposes a list of necessary elements that must be governed for SOA. The items are Service portfolio management, services technical architecture, service design and development, configuration and release management, contract management, service monitoring and control, incident management and change management. However, their set of activities to establish governance of consumer applications is dispersed into several items and does not cover all the aspects described by the other models, such as prioritization and identification of services and solution and security monitoring.

Therefore, this literature review demonstrates that there is a lack of convergence of these proposals regarding to the necessary processes for SOA Governance; due to the gaps and similarities identified, the establishment of a broad approach for effective governance model for Service-Oriented Architecture is an important issue.

III. The CommonGov Approach

The related work presented in Section 2 was analyzed in order to create an approach that consolidates the processes proposed in a common approach, which was named as CommonGov – A Common Governance Model for SOA – presented in Figure 1. Elements were sorted in groups and subgroups, defined accordingly to similarities on their objectives, activities, descriptions and deliverables. The main groups are: strategy, compliance, execution and support. The process descriptions

are presented as follows.

A. STRATEGY GROUP

The strategy group comprises activities to define and manage all necessary principles and goals of the governance model, tailored according to organization needs.

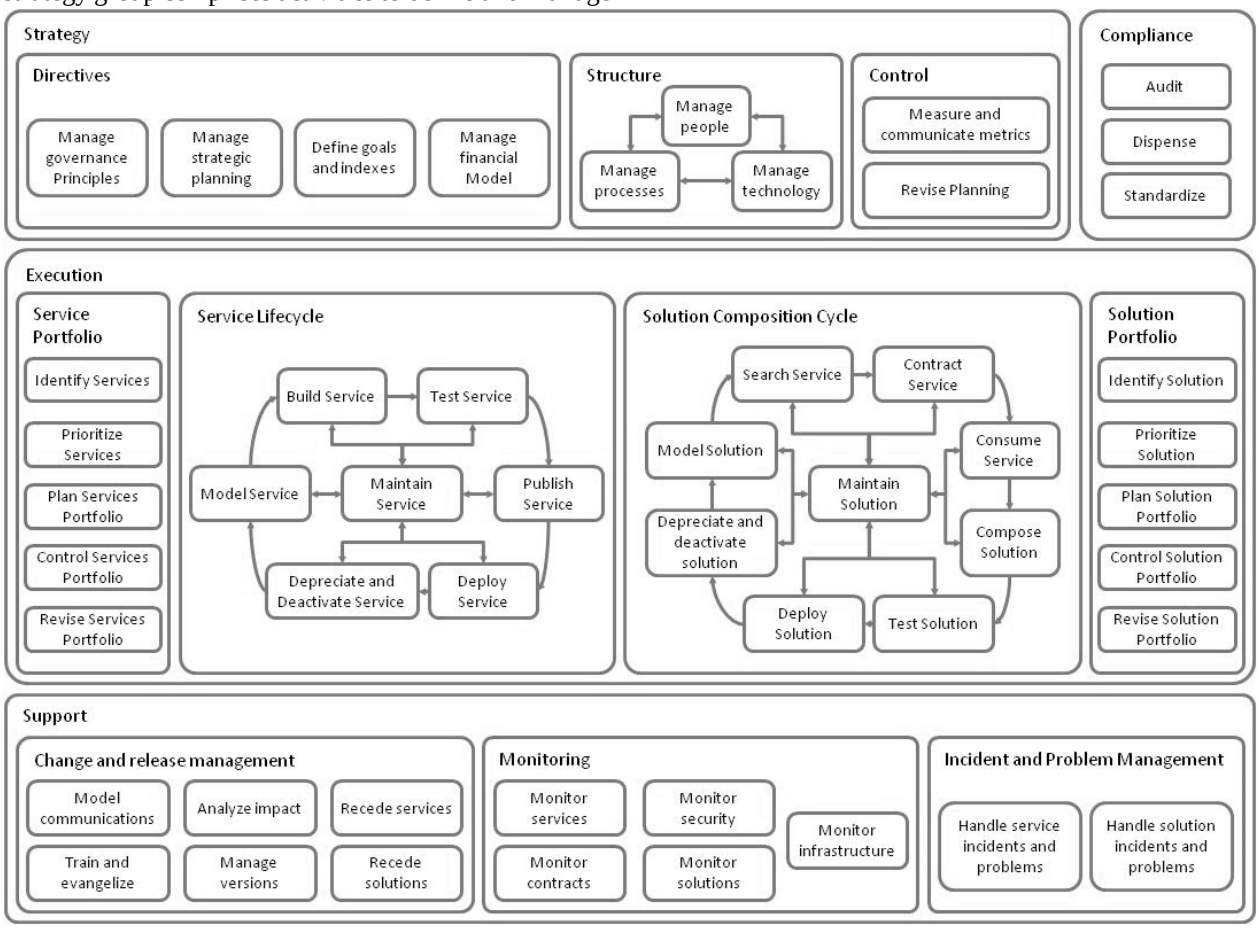

Figure 1. SOA Governance Processes – The CommonGov Approach

It is responsible to define clear guidelines for decision making, work organization and planning activities to establish an incremental implementation of the governance model. The group is divided into tree subgroups: Directive, Structure and Control.

1) Directive: The directive subgroup contains processes to define guidelines to support decisions aligned to business and IT Goals. It is divided in the following process:

(a) Manage governance principles: This process is responsible to establish a list of the business drivers that steers the actions to implement and maintain the service architecture, providing a baseline of directives for management decisions

(b) Manage strategic planning: This process is responsible to define the major milestones and initiatives necessary to implement tools, processes and teams for operating the SOA structure. These actions are structuring projects and they are not operational actions. They provide a roadmap for SOA implementation in the organization

(c) Definition of goals and metrics: This process is responsible to define items to measure the success or failure of the strategic planning and the execution of the operational processes, providing tools to verify if the SOA implementation is aligned with the business goals.

(d) Manage financial model: This process is responsible to define the accountabilities for funding of strategic initiatives and for building and operation of services and SOA solutions. An important step in this process is the decision of the one responsible to the payment of service construction - a decision between payment by the first consuming application or by a dedicated budget for service construction is an example of concern that should be handled in this step. Marks and Bell [17] present some insights in this direction.

2) Structure: The structure subgroup defines the necessary resources and standards that must be implemented in the organization at each of the strategic planning milestones. It consists of three processes:

(a) Manage People: This process is responsible to define the human resources and their organization in roles, accountabilities and skills. It is also responsible to establish the format and the evolution of the organization structure that is necessary to implement SOA. Besides, it provides drivers for training and evangelization processes;

(b) Manage Processes: This process define what processes should be implemented at each phase of the plan. According to several authors ([3], [4] and [6]), SOA governance should be implemented in a incremental strategy. This manage process defines which of the CommonGOV processes should

be implemented in each deployment interaction;

(c) Manage Technology: This process is responsible to define the set of tools that should be deployed at each step for SOA establishment.

3) Control: This subgroup contains the processes necessary to obtain measures and adjust the strategic plan due to the obtained results. It consists of two processes:

(a) Measure and communicate metrics: This process is responsible to periodically gather data, and evaluate the governance system metrics. The evaluation is performed comparing the collected metrics to the goals. The results produced from a critical analysis are then transmitted to stakeholders;

(b) Revise planning: This process is responsible to periodically update the plan and all strategy variables based on the achieved results, Consequently, proposal of changes to the elements defined by the strategy group processes are defined.

B. COMPLIANCE GROUP

This group contains processes necessary to enforce alignment of the SOA initiative to the business goals. It is composed by three processes, with no subgroups. These processes can be integrated within similar processes that already exists in the organization resulting from another existing quality or auditing model.

1) Audit: This process is responsible to define all activities necessary to establish periodic audits to verify compliance with standards and principles that are defined in the governance model.

2) Dispense: This process is responsible to handle all requests of non-conformity with the model, establishing activities to execute the analysis, justification and control of the identified deviations. It also handles assessment of risks conducted by the stakeholders.

3) Standardize: This process define the activities to establish, review, approve, publish and retire standards. It also ensures that these standards are auditable and periodically communicated to the relevant stakeholders.

C. EXECUTION

This group contains processes necessary to build and control service-oriented solutions. It considers four subgroups: service portfolio, service lifecycle, service composition cycle and solution portfolio.

1) Service Portfolio: This subgroup contains the processes required to manage service portfolio. This portfolio includes: the services planned to be developed; the available services currently executing in the operational scenario; the services marked as depreciated, which are waiting to be put out; and the retired services, which are not available to be invoked. The processes of this group are organized in a way that stakeholders can have a precise view of the corporate services roadmap. It contains five processes:

(a) Identify services: This process is responsible to identify and evaluate the candidate services identified from business processes and business requirements. Erl [2] defines a candidate service as an abstract (not implemented) service which, during the design phase of a service lifecycle model, could be chosen to be implemented as a physical service (e.g., a web service) or as a function of a traditional application. The activities of this process are responsible to measure service candidate value and accordingly to include them in the service portfolio. Examples of approaches to conduct this step is the proposals of Azevedo et al [18] and Leopold and Mendling [19]

(b) Prioritize services: This process is responsible to define the priority of each service for the enterprise, considering return of investment, criticality, and organization strategic initiatives. The approach of Azevedo et al.][20] can be used for prioritization.

(c) Plan service portfolio: This process is responsible to manage a high level plan of services for construction, evolution or depreciation, considering costs, business strategy and deadlines of each initiative.

(d) Control service portfolio: This process is responsible to measure adherence to the plan and to perform the required actions in the case of deviations.

(e) Revise service portfolio: This process is responsible to periodically review the portfolio and reprioritizes its elements.

2) Service Lifecycle: This subgroup is the core of the governance model and deals with the service development lifecycle processes, considering all the necessary activities for service development starting from modeling and going to deployment and maintenance. This subgroup is composed by seven processes. Some approaches that comprises this processes are the proposals of Papazoglou and Heuvel [21], Bianculli et al. [22] and Pfeffer et al. [23]

(a) Model service: This process is responsible to define activities for service modeling, considering all aspects to define service contracts. The approach presented by Azevedo et al. [24] or Rahmani et al. [25] approaches. Both of the approaches propose to use UML diagrams for service modeling. The principles proposed by Erl [26] can also be in this step.

(b) Build service: This process is responsible to comprise activities for building services. It can use several standards, aiming to provide guidelines for each programming language or technology in use by the organization to develop services. The approach presented by Azevedo et al. [24] for service development can be used in this step.

(c) Test service: This process define the activities required to test services, considering all aspects of a service contract, including unit, assembly, functional, load and security tests and SLA evaluation. One important point in this process is the validation of the contract by the service owner, ensuring that the service is compliant with its planned business functionality. Another important step is the validation with external partners in distributed scenarios, considering that the service is suitable for inter-organization operation. The proposals described in the work of Canfora and Di Penta [27] can be used in this step. They present a survey in the services test area, in addition of approaches of unit test, integration test, non-functional test and regression test. Besides Baresi

and Dinito [28] also present approach for service analysis and testing.

(d) Publish service: This process is responsible to defines activities to publish the services in registries, enterprise service bus and any other service management tool that must be developed and/or configured before making the service available for consumption. Activities of this process include documentation provision and also the definition of mechanisms for service dynamic binding. The approach proposed by Arnold et al. [29] is an example of approach that could be used to define the activities of this step.

(e) Deploy service: This process is responsible to define the activities for deployment of services on each environment that composes the organization landscape. Arnold et al. [29] propose to employ models-based standards using formal methods that represent deployment topologies. Their approach can be used in this step depending on the organization requirements towards model-based approaches.

(f) Depreciate and deactivate service: This process is responsible to define activities to depreciate and withdraw a service. It also comprises activities to communicate to and negotiate with service consumers about the updates on service status. Josuttis [30]presents some activities to depreciate and deactivate services.

(g) Maintain service: This process comprises activities to evolve and perform maintenances (e.g., bug fixes) on services. It also includes actives to communicate and negotiate with relevant stakeholders the changes on service status.

3) Solution Composition Cycle: This subgroup handles the necessary processes to define service-oriented solutions and regulate service consumption and composition. It addresses the following processes:

(a) Model solution: This process is responsible to establish activities to model service-oriented solutions, considering tasks like distributed processing, composition, distributed transactions and adherence to contracts.

(b) Search service: This process is responsible to define activities to guide the service search on service repositories.

(c) Contract service: This process comprise activities to request authorization, to establish agreements on SLA variables and to ensure that the contracted service fulfills the solution requirements;

(d) Consume service: This process is contains the activities that a consumer must execute to access a service endpoint, including security and technical requirements.

(e) Test solution: This process is responsible to define the steps for executing a black-box test of the solution, including the validation of the consumed services fitting in the solution architecture and also the assessment of the compliance of the service with the solution requirements.

(f) Deploy solution: This process comprises the activities for deployment of composite solutions, considering their distributed characteristics and addressing any new issue in the SOA context.

(g) Depreciate and Deactivate solution: This process is responsible to depreciate or deactivate a solution, including the notification to the service provider the disposal of resources that had been used to consume the service due to the end of the contract.

(h) Maintain solution: This process is responsible to define the activities to evolve or maintenance of services. In particular, it includes the steps that must trigger any kind of contract realignment between service consumer and provider.

4) Solution Portfolio: This subgroup defines the processes that regulate the definition and evolution of a SOA Solution Portfolio. The solution portfolio is similar to the service portfolio, but it handles the solutions that consume the services. The solution portfolio is dependent of the service portfolio. Both portfolios must be managed in an aligned way. It considers four processes:

(a) Identify solution: This process comprises activities to identify and evaluate the value of candidate SOA solutions, based on business processes and organizational demands. This process should be aligned with any existing enterprise architecture or application consolidation projects to ensure a controlled and convergent evolution of the roadmap of applications of the organization.

(b) Prioritize solution: This process contains activities to prioritize building, maintenance and disposal of SOA solutions, based on the status of both the service and solutions portfolios.

(c) Plan solution portfolio: This process comprises activities to define milestones of actions that must be executed over the portfolio's elements, like construction, evolution or depreciation

(d) Control solution portfolio: This process defines the activities required to measure adherence to plan and act on deviations considering changes in the solution and service portfolios.

(e) Revise solution portfolio: This process comprises the required activities to periodically review the portfolio, based on the business strategy and the service portfolio evolution.

D.SUPPORT

This group considers all the processes necessary to support the establishment of SOA. It activities ranges from cultural aspects to runtime concerns. It is divided into three groups:

1) Change and Release Management: This subgroup addresses the issues related to changes in the environment, handling changes in culture, people skills and technical components. It comprises six processes.

(a) Model communications: This process is responsible to define all activities related to communication between service providers, consumers and stakeholders. It comprises the definition of communication matrixes, channels and events that triggers notifications between involved parties and definition and standardization of the format of each notification or message.

(b) Train and evangelize: This process comprises activities to enhance skill and improve SOA culture in the organization. Skills must be improved in technical and process domains while evangelization must be executed in IT and business areas.

(c) Analyze impact: This process contains the necessary activities to identify impacts, risks and actions resulted from a

change in technical and business perspectives and to interfere on service and solution portfolios due to changes.

(d) Manage versions: This process considers all activities necessary to establish a version control policy. They should guide the behavior of depreciation and deactivation processes of service and solution lifecycles and must define criteria for decision if a new version of service must overwrite the existing one or must coexist with it.

(e) Recede services: This process contains the activities to periodically retest the built service portfolio to check eventual contract breaking by the service provider and avoid operational problems to the consumers;

(f) Recede solutions: This process comprises activities to periodically retest SOA Solutions to check eventual contract breaking from consumers and avoid operational problems on services due to unexpected behavior of a consumer.

2) Monitoring: This group addresses the necessary processes and responsibilities to monitor the consistency of the service architecture. It is composed by five processes:

(a) Monitor services: This process is responsible to monitor the integrity of the services, verifying availability and reporting business and technical errors identified during operation. The approach of Bluemke and Warda [31] is an example of approach to be used in this step. They propose to use a module for service monitoring in the organization's Enterprise Service Bus (ESB). ESB is the core technology in an SOA initiative [32]

(b) Monitor contracts: This process comprises activities to monitor fulfillment of contracts, evaluating functional and nonfunctional variables and alerting eventual changes in patterns of consumption of services.

(c) Monitor security: This process contains specific activities to verify security of the architecture, observing not only the isolated services, but also correlating information to identify possible security problems to the entire architecture. This process gains importance due to the possibility to constitute service-oriented solutions that consumes services from other organization through the Internet, constituting an Internet of Services [13]. It brings new challenges related to security requirements, like inter-organization authentication and attack protection.

(d) Monitor solutions: This process is responsible to define the processes to check the integrity of solutions and to check the predicted behavior of compositions, including transaction monitoring, allowing the check the behavior of each service due to the execution of distributed transactions. Tripathy and Patra[33] proposes an approach to monitor service based solutions that addresses this concern;

(e) Monitor infrastructure: This process is responsible to control the status of the infrastructure components of the solution, like servers, databases and application servers that supports the services and SOA solutions, providing a unified view of the resources used by the solutions.

3) Incident and Problem Management: This group comprises the processes to handle incidents and problems detected by users and by monitoring. We can consider issues ranging from technical aspects, like operational errors, to requirement issues, like an SLA failure. The most important issue on this group is not related with how the activity is done, but with who executes the activity. It is composed by two processes:

(a) Handle service incidents and problems: This process defines activities and responsibilities for solving incidents and problems existing on services.

(b) Handle solution incidents and problems: This process is responsible to define the activities and responsibilities for solving incidents and problems identified on SOA solutions.

IV. Comparison and Gap Identification

This section presents a comparison between the most relevant proposals of governance models (selected from the related work presented in Section II) and CommonGov showing the gaps and similarities between them.

The models were selected considering different perspectives:

(i) Academic: Hojaji and Shirazi [6] and Janiesh et al. [13] proposals were selected for this perspective. Niemann et al. proposal [3] was not selected because it presents building blocks in high level of abstraction, and does not address the necessary processes;

(ii) Software vendor: Bennett proposal [8] was selected for this perspective; and

(iii) Consulting company: Manes proposal [11] was selected for this perspective.

The comparison of those proposals and CommonGov results are presented in Table I, and described as follows.

The columns of Table I represent the evaluated governance models and the rows represent each CommonGov process. Each cell, corresponding to the relation Process × Model, describes the presence of a specific process of CommonGov in the related work model, according to the following criteria.

- T (Total): represents that there is a process in the related work model that is completely equivalent to a process proposed in the CommonGov model.
- P (Partial): represents that there is a process in the related work model that includes part of the activities of the proposed process in the CommonGov model.
- N (None): represents that there is no process in the related work model that is equivalent to a CommonGov proposed process.

To evaluate the similarity between CommonGov against the proposed models, Model Coverage and Process Consensus which are described as follows.

1) Model coverage: It shows the degree of similarity of the related work models related to CommonGov. It corresponds to two percentages:

(i) Total Coverage criterion (%): percentage of the related work processes that are present and completely equivalent to CommonGov processes. The results of this criterion are presented in the penultimate line of Table I.

(ii) Partial Coverage criterion (%): percentage of related work processes that are present and partially equivalent to CommonGov processes. The results of this criterion are presented in the last line of Table I.

Group	Subgroup	Process	Open Group	Gartner	Janiesch et al	Hojaji Shiraji	Oracle	Consensus
SOA Strategy	Directives	Manage governance principles	T	P	T	T	T	100%
		Manage strategic planning	N	N	N	T	N	20%
		Define goals and indexes	T	P	T	P	T	100%
		Manage financial model	T	T	T	T	T	100%
	Structure	Manage people	T	P	P	T	T	100%
		Manage processes	T	P	P	T	T	100%
		Manage technology	P	P	P	P	P	100%
	Control	Measure and communicate metrics	P	N	T	P	P	80%
		Revise planning	P	N	P	T	P	80%
Compliance		Auditing	T	P	T	T	N	80%
		Dispensation	T	P	N	N	N	40%
		Standardization	P	P	P	P	N	80%
Execution	Service Portfolio	Identify services	P	N	N	T	N	40%
		Prioritize services	T	N	T	P	P	80%
		Plan service portfolio	T	P	P	P	P	100%
		Control service portfolio	T	P	T	P	P	100%
		Revise service portfolio	T	T	P	P	P	100%
	Solution Portfolio	Identify solutions	T	P	N	N	P	60%
		Prioritize solutions	T	P	N	N	P	60%
		Plan solution portfolio	T	P	N	T	P	80%
		Control solution portfolio	T	P	N	T	P	80%
		Revise solution portfolio	T	P	N	T	P	80%
	Service Lifecyle	Model service	T	T	T	T	T	100%
		Build service	T	T	T	T	T	100%
		Publish service	T	T	T	T	T	100%
		Deploy service	T	T	T	T	T	100%
		Depreciate and deactivate service	P	T	T	N	P	80%
		Maintain service	T	T	T	T	P	100%
	Solution Composition Lifecycle	Model solution	T	N	N	N	P	40%
		Search service	T	N	N	N	P	40%
		Contract service	T	T	N	N	P	60%
		Consume service	T	T	N	N	P	60%
		Compose solution	T	N	N	T	P	60%
		Test solution	T	T	N	N	P	60%
		Deploy solution	T	N	N	N	P	40%
		Depreciate and deactivate solution	P	P	N	N	P	60%
		Maintain solution	T	N	N	N	P	40%
Support	Change and Release Mgmt	Model communications	P	T	P	T	P	100%
		Train and evangelize	P	P	N	N	T	60%
		Analyze impact	T	T	T	T	P	100%
		Manage versions	T	T	P	P	P	100%
		Recede services	N	N	P	P	N	40%
		Recede solutions	N	N	P	N	N	20%
	Monitoring	Monitor services	T	T	T	T	P	100%
		Monitor security	N	N	T	T	P	60%
		Monitor contracts	T	T	T	T	P	100%
		Monitor solutions	T	T	N	N	P	60%
		Monitor infrastructure	N	N	T	P	N	40%
	Incident and Problem Mgmt	Handle service incidents & problems	T	T	P	T	P	100%
		Handle solution incidents & problems	T	T	N	N	N	40%
Model Coverage - Total criterion (%)			72%	38%	36%	46%	20%	
Model Coverage - Partial criterion (%)			18%	34%	24%	22%	62%	

Table 1. Process Comparison Table

To evaluate the Model Coverage, for the total coverage criterion, we count the total presence of the related work model processes compared to Commongov processes. In other words, it is represented by the count of "T" in the

corresponding related work column divided by the number of CommonGov processes. As an example, considering the Open Group model (forth line of Table I), the Total Coverage is equal to 72%. It represents that 72% of the processes proposed by Open Group correspond totally to the processes proposed by CommonGov.

To analyze Partial Coverage, we count the occurrences of partial presence (letter "P") and divide this number by the number of processes. Considering the Open Group model, the Partial Coverage is equal to 18%. It represents that 18% of the processes proposed by Open Group correspond partially to the processes proposed by CommonGov.

2) Process consensus: It aims to identify the percentage of consensus of the Governance processes among the related work models. In other words, it presents if Commongov process is presented in the related work proposed processes. This criterion is computed, for each CommonGov process, as the sum of count of T and the count of P divided by the number of related work models. The results of this criterion are presented in the last column of Table I.

As an example, in the case of "Manage governance principles", there are four "T" and one "P", and five related work models. So, the percentage is 100%. So, this process is considered important to SOA Governance according to the evaluated models.

Group	Subgroup	Process Consensus
SOA Strategy	Directives	80%
	Structure	100%
	Control	80%
Compliance		67%
Execution	Service Portfolio	84%
	Solution Portfolio	72%
	Service Lifecycle	97%
	Solution Composition Lifecycle	56%
Support	Change and Release Management	66%
	Monitoring	72%
	Incident and Problem Management	70%

Table 2. Average Process Consensus by Subgroup

Subgroup	Process	Open Group	Gartner	Janiesch et al	Hojaji Shiraji	Oracle
Monitoring	Monitor Services	T	T	T	T	P
	Monitor Security	N	N	T	T	P
	Monitor Contracts	T	T	T	T	P
	Monitor Solutions	T	T	N	N	P
	Monitor Infrastructure	N	N	T	P	N

Table 3. Analysis of Monitoring Subgroup

On the other hand, in the case of "Manage strategic planning", there are only one "T" for five related work models which results on 20%. It means that this process is not identified by the related work as a relevant one.

Another important analysis is to consider the group and subgroup importance. It corresponds to the average consensus of the processes present in the group/subgroup, and is presented in Table II. To calculate this value, we compute the average of the process consensus. For example, the subgroup Directive of SOA Strategy group has three processes with 100% of consensus and one process with 20% of consensus, as presented in Table I. It results on 80% of consensus of the subgroup "SOA Strategy/Directives" in Table II. The comparison of this data resulted in the following findings:

• Processes of the sub-groups Service Lifecycle Management, Definition of Structure, and Service Portfolio Management are well addressed by most of the models. The average consensus of these subgroups is equal to 97%, 100% and 84%, respectively.

• Existing models diverge if it is necessary to govern the composition lifecycle. This fact is expressed by the Process Consensus of the subgroup "Execution/Solution Composition Lifecyle" which is equal to 56% in Table II. In Table I, this fact is presented in more details, and we can notice that The Open Group model [4] and Bennet [8] consider several processes to address this point. In that case, almost all Open Group processes are totally described considering CommonGov, while Bennet [8] processes are more partially described. On the other hand, Hojaji and Shirazi [6] and Janiesch et al. [13] consider only part of corresponding activities, especially the ones for contract negotiation and service consumption.

• There is a consensus that monitoring is an important issue to be addressed by a governance model. The consensus of this subgroup is equal to 72%. However, proposals diverge concerning the elements that should be monitored, as highlighted in Table III. This table summarizes the monitoring subgroup, and presents that all models include

processes for monitoring contracts and services. Among the proposals, Hojaji and Shirazi [6] and Janiesch et al. [13] point to the need of security monitoring, while The Open Group [4] and Gartner [11] emphasize that solutions monitoring is required. Besides, The Open Group [4], Oracle [8] and Gartner [11] consider infrastructure monitoring as a separate discipline which have to be addressed by other levels of governance, like IT Governance.

• The model that includes more processes is the Open Group model: 72% of its processes are completely equivalent to CommonGov processes. However, it is partially equivalent to the processes for change management, strategy evolution and monitoring.

From this analysis we can identify that there is a gap between the approaches that can be addressed by a new governance model, based on the processes that were normalized in this work and presented in Figure 1.

V. Conclusions and Future Work

This work presented an analysis of models proposed for SOA Governance by academia and industry. The results made explicit divergences and similarities among the models, and based on those models it was established a consolidated approach, named as CommonGov – A Common Governance Model for SOA. The proposed processes were sorted in groups and sub-groups, and their definitions were presented. Two metrics were proposed to help the identification of gaps and commonalities: process consensus, that presents the importance of a process in the governance context according to the literature, and model coverage, that presents the coverage of the processes of a model from literature compared to the CommonGov processes.

Similarities appear on processes to manage the service lifecycle and to define principles and organizational units of the governance model. This result comes from the presence of processes of these areas in all analyzed models.

The main divergences are related to the necessity to control the SOA composite solution lifecycle and on aspects of monitoring.

Considering the SOA composition solution lifecycle, this is an important aspect due to the direct relation of SOA benefits to solution composition. According to Erl [2], one of the greatest benefits of SOA is the capacity of composing new solutions by assembling services into composite services and solutions. That means that composition is on the core of a SOA strategy and it is an important variable to be managed and governed.

In the context of monitoring, besides the necessity of specific processes for SOA solution monitoring, that is a direct consequence of the necessity to govern both solutions and services, another important aspect is security. According to Fortis et al. [34], security is the greatest concern to the adoption of service-oriented solutions on cloud environments that yields direct difficulties to develop inter-organization solutions. Therefore, the establishment of processes for service and solution security is an important factor to enable internet based SOA solutions.

The result of this analysis can help further research in SOA Governance on tailoring specific Governance processes to organizations, defining Governance roles, and accounting and specifying case studies. Besides, the proposed metrics can help the evaluation of future SOA governance frameworks proposals.

This work corresponds to one important step towards a complete governance model definition, addressing processes to deploy a successful SOA. In this direction, as future work we propose:

• Execute a survey with SOA experts to check if the divergent processes are relevant in practice;

• Refine the model considering the results of the survey and including roles to each process;

• Analyze the relation between maturity models and SOA Governance processes in order to establish a sequence of steps to instantiate CommonGov in organizations and to define importance of each process to enhance consensus and coverage metrics;

• Apply the proposed process in a real world scenario.

VI. References

[1] M. P. Papazoglou, "Service-oriented computing: Concepts, characteristics and directions", in *Proceedings of the Fourth International Conference on Web Information Systems Engineering*, 2003, p. 3–12.

[2] T. Erl, *Service-Oriented Architecture (SOA): Concepts, Technology, and Design.* Upper Saddle River, NJ, USA: Prentice Hall, 2005.

[3] M. Niemann, A. Miede, W. Johannsen, N. Repp and R. Steinmetz, "Structuring SOA Governance", *International Journal of IT/Business Alignment and Governance*, vol. 1, no 1, p. 58–75, 2010.

[4] The Open Group, *SOA Governance Framework*, 2009. [Online]. Available at: https://www2.opengroup.org/ogsys/jsp/publications/PublicationDetails.jsp?catalogno=c093. [Acessed on: 14-abr-2012].

[5] T. G. J. Schepers, M. E. Iacob and P. A. T. Van Eck, "A lifecycle approach to SOA governance", in *Proceedings of the 2008 ACM symposium on Applied computing*, Fortaleza, CE, 2008, p. 1055–1061.

[6] F. Hojaji and M. R. . Shirazi, "A Comprehensive SOA Governance Framework Based on COBIT", in *Proceedings of the 6th World Congress on Services*, 2010, p. 407–414.

[7] C. Janiesch, A. Korthaus and M. Rosemann, "Conceptualisation and facilitation of SOA governance", in *Proceedings of the 20th Australasian Conference on Information Systems*, Melbourne, 2009, p. 154–163.

[8] S. G. Bennett, *Oracle Practitioner Guide - A Framework for SOA Governance*, 2012. [Online]. Available at: http://www.oracle.com/technetwork/topics/entarch/oracle-pg-soa-governance-fmwrk-r3-2-1561703.pdf. [Acessed on: 03-jul-2012].

[9] W. A. Brown, G. Moore and W. Tegan, *SOA Governance-IBM's Approach*, Effective Governance through IBM SOA Governance Management Method approach, 2006. [Online]. Available at:

ftp://170.225.15.40/software/soa/pdf/SOA_Gov_Process_Overview.pdf.
[10] *Ready to use SOA Governance for Microsoft*. [Online]. Available at: http://www.soa.com/solutions/microsoft/microsoft_and_soa_software/. [Acessado: 17-jun-2012].
[11] A. Thomas Manes, *A Guidance Framework for SOA Governance*, Gartner Group, G00203879, 2009.
[12] M. Niemann, C. Janiesch, N. Repp and R. Steinmetz, "Challenges of Governance Approaches for Service-Oriented Architectures", in *Proceedings of the Third IEEE International Conference on Digital Ecossystems and Technologies*, Instanbul, 2009.
[13] C. Janiesch, M. Niemann and N. Repp, "Towards a service governance framework for the internet of services", in *Proceedings of the 17th European Conference on Information Systems*, Verona, 2009.
[14] H. M. Teixeira Filho and L. G. Azevedo, "CommonGOV: A Consolidate Approach for Governance of Service-Oriented Architectures", *In Proceedings of the 8th International Conference on Web Services Practices*, São Carlos, Brasil, 2012, p. p. 389–394.
[15] *Cobit 4.1*. EUA: IT Governance Institute, 2007.
[16] S. Adams, *ITIL V3 foundation handbook*. The Stationery Office, 2009.
[17] E. A. Marks and M. Bell, S*ervice-Oriented Architecture (SOA): A Planning and Implementation Guide for Business and Technology*, 1st ed. Wiley, 2006.
[18] L. G. Azevedo, F. Santoro, F. Baião, J. Souza, K. Revoredo, V. Pereira and I. Herlain, "A Method for Service Identification from Business Process Models in a SOA Approach", in *Enterprise, Business-Process and Information Systems Modeling*, 2009, p. 99–112.
[19] H. Leopold and J. Mendling, "Automatic derivation of service candidates from business process model repositories", In *Proceedings of the 15th International Conference on Business Information Systems*, Vilnius, Lithuania, 2012, vol. 117.
[20] L. Azevedo, F. Baião and F. Santoro, "A Business Aware Service Identification and Analysis Approach", *In proceedings of the International Conference Information Systems*, Avila, Spain, 2011, p. 11–13.
[21] M. P. Papazoglou and F. Van Den Heuvel, W., "Service-oriented design and development methodology", *International Journal of Web Engineering and Technology*, 2006.
[22] D. Bianculli, C. Ghezzi, and C. Pautasso, "Embedding continuous lifelong verification in service life cycles", *in Proceedings of the 2009 ICSE Workshop on Principles of Engineering Service Oriented Systems*, 2009, p. 99–102.
[23] H. Pfeffer, D. Linner, I. Radusch and S. Steglich, "The bio-inspired service life-cycle: An overview", in *Proceedings of the 3rd International Conference on Autonomic and Autonomous Systems*, 2007.
[24] T. Diirr, L. G. Azevedo, F. Faria, F. Santoro and F. Baião, "Practical Approach for Service Design and Implementation", In *Proceedings of the IADIS International Conference Information Systems*, Berlin, Germany, 2012, p. 197–204.
[25] A. T. Rahmani, V. Rafe, S. Sedighian, and A. Abbaspour, "An MDA-Based Modeling and Design of Service Oriented Architecture", in *Computational Science*, 2006, p. 578–585.
[26] T. Erl, *SOA Principles of Service Design*, 1st ed. Prentice Hall, 2007.
[27] G. Canfora and M. Di Penta, "Service-oriented architectures testing: A survey", In *Lecture Notes in Computer Science*, vol. 5413, p. 78–105, 2009.
[28] L. Baresi and E. D. Nitto, *Test and Analysis of Web Services*. Springer, 2007.
[29] W. Arnold, T. Eilam, M. Kalantar, A. V. Konstantinou and A. A. Totok, "Pattern based SOA deployment" In *Lecture Notes in Computer Sciences*, vol. 4749, 2007.
[30] N. Josuttis, *Soa in practice*, 1st ed, O'Reilly, 2007.
[31] I. Bluemke, M. Warda and A. Derezińska, "Monitoring services on Enterprise Service Bus", In *International Journal on Computer Science and Information Systems*., vol. 3, no 1, p. 1–13, 2008.
[32] E. Hewitt, *Java SOA Cookbook*. O'Reilly Media, Inc., 2009.
[33] A. Tripathy and M. Patra, "Service Based System Monitoring Framework", *International Journal of Computer Information Systems and Industrial Management Applications*, vol. 3, p. 924–931, 2011.
[34] T.-F. . b Fortiş, V. I. . b Munteanu and V. . b Negru, "Towards a service friendly cloud ecosystem", in *Proceedings of the 11th International Symposium on Parallel and Distributed Computing*, 2012, p. 172–179.

Author Biographies

Haroldo Maria Teixeira Filho is integration and information architect on Petróleo Brasileiro S/A and student of the Graduate Program in Informatics at UNIRIO. Electronic Engineer by UFRJ in 1997, postgraduate in System Analysis by PUC-RJ in 2001 and MBA in Enterprise Management by FGV in 2006. His research areas include service-oriented architecture and computing, business process management, IT governance and strategy, systems integration and information management.

Dr. Leonardo Guerreiro Azevedo isis Professor with the Applied Informatics Department at Federal University of the State of Rio de Janeiro (UniRio), Brazil. He is member of Graduate Program in Informatics at UniRio (PPGI/UNIRIO). His research areas include Service-Oriented Architecture, Business Process Management, Business Rules, Management and Execution of Authorization Rules, Role-Based Access Control, Spatial Database, Approximate Query Processing, and Model-Driven Architecture. His research has been published, among others, in NWeSP, ICEIS, ECIS, BPMDS, SOSE, IADIS Applied Computing, RESI, GeoInfo, JIDM, Brazilian Symposium in Information Systems, and IADIS Information Systems. He is a board member of Brazilian and international program committees.