

# The Portuguese government cloud services, deployment and management framework

José A. Cordeiro Gomes <sup>1</sup>, Luisa Domingues <sup>2</sup>

1) DCTI / ISCTE-IUL / ISTA / ADETTI-IUL; GeRAP, Lisboa, Portugal

[Cordeiro.Gomes@iscte.pt](mailto:Cordeiro.Gomes@iscte.pt)

2) DCTI / ISCTE-IUL / ISTA / ADETTI-IUL, Lisboa, Portugal

[Luisa.Domingues@iscte.pt](mailto:Luisa.Domingues@iscte.pt)

## Abstract

In the context of shared services implementation within the Portuguese public administration a new initiative named Governmental Open Cloud (GO-Cloud) has emerged. The GO-Cloud initiative implementation overlays the double objective of establishing a technological platform that will leverage the shared services adoption spreading among public administration entities, concerning both the already deployed financial and budgetary management solution and the shared human resource management solution, and the provisioning of ICT resources and services in a more flexible and effective way.

The Portuguese shared services solution is based on a service oriented architecture which facilitates the adoption and integration of the cloud computing paradigm and the relating short term expected economical and structural benefits concerning both governmental efficiency and effectiveness. Two of the major risks concerning GO-Cloud are the relative lack of maturity of cloud computing technology and standards as well as the cultural and organizational change it introduces within public administration universe of more than 510000 employees. In order to properly deal with these threats two initiatives have been taken: (i) at the technical level to build an open cloud based on existing technologies and interconnection standards; (ii) at the management level to develop a governance model able to address and support its implementation, development and management.

This paper focuses in both aspects: the GO-Cloud services architecture and its respective deployment and governance models. The deployment model is inspired in the web services paradigm and the management model deploys the Shared Services Analysis Model (SSAM) to the cloud in a three layer management approach (strategy, business and operation).

**Keywords:** *Government Cloud; Shared Services; Cloud Deployment Model; Cloud Management Model; SSAM*

## 1. Research context

As an outcome of the central public administration restructuring program (*Programa de Reestruturação da Administração Central do Estado, in short PRACE*) [PRACE 2006], in 2007 the Portuguese government launched an initiative to implement financial, including budgetary, and human resources shared services management within the central public administration, covering a population of around 510.000 employees working in 360 public entities. This goal

was endorsed to GeRAP [GeRAP 2007], a new public company owned by the Ministry of Finances (and Public Administration) (MF)<sup>1</sup>.

Also as an outcome of PRACE, the agency for the administrative modernization (*Agência para a Modernização Administrativa*, in short *AMA*) was created by the end of 2006, depending directly on the prime minister and aiming to identify, develop and evaluate programs, projects and initiatives that lead to a more efficient and up-to-date public administration. AMA owns the public administration interoperability platform.

AMA and GeRAP share a common goal: to reach a more integrated and efficient public administration.

Since May 2007 GeRAP has been working in a shared services program, named GeRALL. Figure 1 presents a high-level view of GeRALL main components. It encompasses a set of five integrated solutions: (i) GeRFiP which concerns financial shared services management; (ii) GeRHuP which concerns human resources shared services management; (iii) GeADAP which relates with the integrated evaluation of public administration services, managers and workers; (iv) GeDM which concerns the management and deployment of master data; and (v) GeSBI which offers both a platform and a set of integrated Business Intelligence solutions.

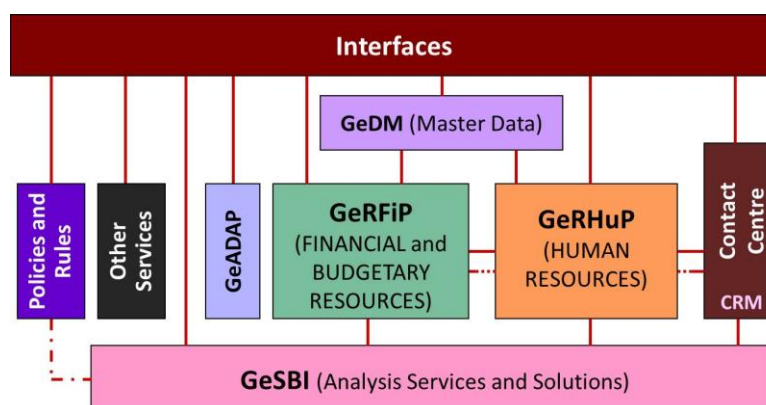


Figure 1 - GeRALL high-level architecture

GeADAP and GeRFiP solutions are already available and operational. GeRHuP is still under development. The first release of GeSBI, focused on financial data, is also available and has been running since last summer. GeDM is the solution that manages public administration reference data. It is already working together with GeRFiP and by the end of the current year it will integrate with GeRHuP.

At this stage, and in order to quickly and consistently deploy these solutions, the existence of a scalable and resilient infrastructure, supported by automated mechanisms and services (e.g., provisioning, deployment and support) became a critical success factor (CSF) [J. F. Rockart 1981].

The quality of infra-structure services is crucial for the success of GeRAP and AMA missions as well as for the reduction of public administration IT costs. Therefore these two structures decided to join competences and efforts in order to provide information and communication technology (ICT) shared services for the overall public administration and launch a new program concerning the deployment of a Portuguese government open cloud (GO-Cloud). This

<sup>1</sup> The Portuguese Government recently launched a new restructuring program for the central public administration (PREMAC) and has just announced the decision of reducing in 40% the number of central public entities.

paper presents this initiative focusing on the cloud services reference architecture and the adopted management model.

## **2. Public Administration ICT characterization**

Most public entities have typically developed their own silos of information repositories which are usually exacerbated further with an infrastructure that is not well designed to either gather or move information to the appropriate destinations. The need of a global accepted ICT reference architecture, defining interconnectivity standards, together with the lack of a unique master data catalogue are two of the main sources for data integrity problems. Thus, the public ICT infrastructure may be characterized as follows: Culture of autonomous applications, owned, developed and maintained by the proper public entity; existence of multiple data centres even within the same ministry, some of them very small; dispersed acquisitions; communication infrastructures not fully integrated even within some of the ministries; lack of ICT professionals to internally operate and maintain applications and systems (recruitment has been frozen some years ago and offered wages for some of the IT professionals categories are not market competitive); need to improve Quality of Service levels (more reliability and better performance); low level of integration among systems; management of outside access not integrated, which increases security risks and costs. According to a study developed by the General Inspection of Finances [IGF 2009], dated December 2009, the reorganization of the central public administration back-office could have saved around € 63 million.

## **3. Why a Cloud for the Portuguese Government?**

Cloud computing represents a new business model to deliver computing resources. Nowadays there are several definitions of cloud but we have adopted the National Institute of Standards and Technology (NIST) definition of Cloud Computing which characterizes it as “a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction” [Mell et al. 2009].

According to NIST the cloud may be deployed in four different models – Private, Community, Hybrid or Public cloud – and offers three service models: Infrastructure as a Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). Each service model may encompass different service classes.

The governmental cloud is an opportunity to solve some of the previously enounced problems and requirements, promoting rationalization and standardization of resources, data, applications and services. It provides a higher control and transparency with IT costs as well as the basis for the construction of the “public administration data warehouse”.

The GO-Cloud initiative is intended to:

- Provide a stable, manageable, properly structured infrastructure to GeRAP own internal shared service solutions;
- Accelerate the pace at which the government will realize the value and adopt cloud computing by requiring agencies to evaluate safe and secure cloud computing options before making any new investments.

The main challenges to overcome with the government cloud initiative include faster delivery procedures, a more efficient use of computational resources, increased levels of standardization and quality-of-service, global introduction of both new computing paradigms and public administration standard solutions, lower ICT total costs of ownership, leveraging the economy

of scale, and the achievement of a more proficient procurement. Just by adopting virtualization and business applications sharing we expect small and medium public entities (300 workers or less), that represent more than 75% of the central Portuguese administration public entities, to reduce the concerned hardware and licensing costs in more than 60%.

Although the expected benefits are significant, caution must be taken in what concerns privacy, security, data location and risk of loss of control. Special attention must be given to the low level of maturity of nowadays clouds technology.

Security is a major issue the cloud needs to properly address [L. Martin 2010]. Actually security measures are cheaper if implemented on a larger scale (e.g. filtering, patch management, access control and hardening of virtual machine instances) and more efficient when centrally managed [ENISA 2009]. The six security functions to be considered by the GO-Cloud are: identity management; information security; application security; infrastructure security; security monitoring; and compliance monitoring.

It is broadly accepted that security in cloud tends to be as good or even better than in the traditional systems, in part because providers are able to devote resources to solve security issues that many customers cannot afford. However, the complexity of security is greatly increased when data are distributed over a wider area or greater number of devices and in multi-tenant systems that are being shared by unrelated users. Private cloud installations are in part motivated by users desire to retain control over the infrastructure and avoid losing control of information security.

Another aspect to consider is the increasing level of integration among systems and services required by the cloud. One of the cloud working areas concerns the development and deployment of integration services components, including middleware solutions, in order to achieve reliable and secure integration of resources, data and services, according to the defined standards. This concern also refers to the integration and interoperability with other clouds as well as service brokerage provisioning.

As far as cloud is concerned special attention must be given to data, its location as well as privacy. The cloud state-of-the-art technology and standards cannot assure data in public clouds may not be accessed and copied by others. Furthermore, the lack of suitable legislation creates other types of difficulties such as contract definition and management once the legal environment is not clear enough and leads to agreements that are impossible to fully monitor. Another major issue is the impossibility to assure that data once erased are effectively destroyed.

Therefore it is important to classify data and define a storage policy accordingly. Another important aspect is to progressively promote and implement standards within the cloud or in the relationship with other clouds, allowing interoperability, facilitating accessibility and reducing lock-in mechanisms. In one word be opened.

For those reasons we believe the best solution for large companies and for governments are private clouds. These clouds must be opened and suitably managed so that they can incorporate both new legal or business requirements as well as technical evolutions provided by public or other private clouds.

#### **4. GO-Cloud requirements definition**

Actually government cloud means moving from a public ICT infrastructure which was planned, procured and managed separately by public entities, to a new model in which ICT infrastructure is centrally provided and managed as a shared utility. It is a new government shared service.

By leveraging shared infrastructure and economies of scale, cloud computing presents a compelling business model for the public administration. Agencies will be able to measure and

pay for only the IT resources they consume, increase or decrease their usage to match requirements and budget constraints, and leverage the shared underlying capacity of IT resources via a network. Resources needed to support mission critical capabilities can be provisioned more rapidly and with minimal overhead and routine provider interaction.

The following set of global requirements was considered in the high-level design of the solution: Provision of IaaS, PaaS and SaaS services. IaaS offer must include both high-end and low-end service levels in order to address different needs of usage. Other requirements the GO-Cloud solution must consider and explore are self-service mechanisms with approval workflows; automated provisioning; pay-per-use with clear utilization periods; easy scalability; integration with other clouds; reuse of current infrastructure whenever possible. Later on other types of solutions like Business Processes-as-a-Service (BPaaS) will be envisaged.

The previously enunciated CSF, the set of cloud requirements as well as the cloud computing state-of-the-art framed the decision of implementing a Government Open Cloud (GO-Cloud) based on existing standards, able to integrate other clouds, private or public.

Another critical aspect to consider relates to the GO-Cloud governance model which must be able to federate the main public administration ICT entities.

Four major concerns have been envisaged: (i) the need to broadly deploy shared services, which require scalable, flexible and reliable ICT infrastructures with high quality-of-service levels; (ii) the opportunity to improve standardization and interoperability levels among public systems; (iii) the ability to improve the quality of ICT services, enhance security levels and reduce costs; and, (iv) the capacity to deploy and enhance new computing and business paradigms.

Considering both requirements and current maturity stage of cloud computing solutions the decision was to build a hybrid cloud developed around a private government open cloud. The scope of this initiative is first the central public administration and afterwards both local administration and regional administrations. To anticipate future needs, the evolution of the ICT technology and new market offers, the GO-Cloud must natively take into account the possibility of integration of other public or private cloud services, leveraging both offered services quality and cost competition. Although promising, we must be aware that cloud computing technology is not sufficiently mature yet to be adopted by a government without precautions, being one of the main threats the existing lack of standardization and security which difficult interoperability among different clouds and potentiate lock-in mechanisms.

## **5. GO-Cloud offered services**

As presented in Figure 2 the cloud offers a set of identified services, organized according to the three service models – SaaS, PaaS and IaaS – and supported by a Dynamic Data Centre.

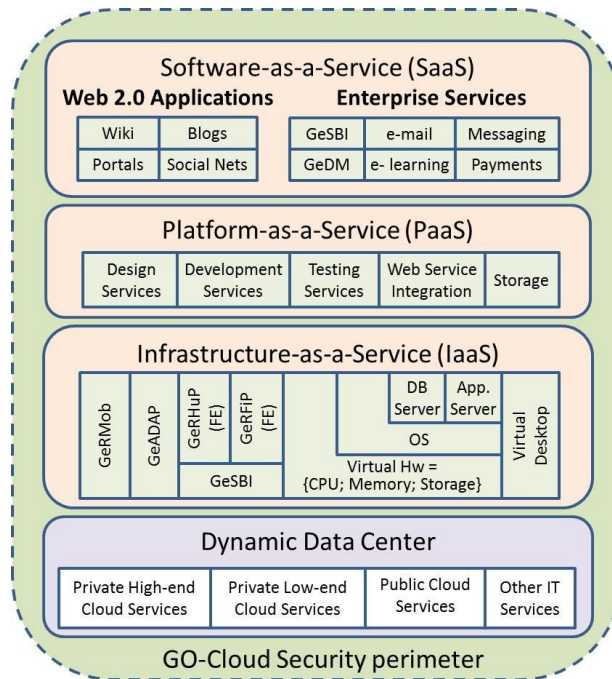


Figure 2 - GO-Cloud Services

In terms of the Dynamic Data Centre offer, and considering that not all applications have the same degree of criticality or require the same level of service, two virtualized infrastructure types of solution will be offered: (i) the high-end, designed to be fault-tolerant and to run 7x24; and (ii) the low-end, addressing to those services that are stateless and may accept maintenance service breaks.

Typically, state-full type of applications such as GeRFiP is addressed by the GO-Cloud high-end offer.

Not all services presented in Figure 2 have the same priority and level of maturity; therefore they will be deployed in a progressive way. Regarding the maturity aspect of today's cloud technology, the priority goes to IaaS, to take advantage of virtualization techniques. The existing SOA and multi-tenant applications such as GeSBI may benefit from SaaS service model, but a significant work is required in order to migrate most of the existing solutions and applications to this new paradigm. The services proposed by the Platform-as-a-Service classes will be carefully and gradually implemented and evaluated, beginning by the development and testing platforms.

The interoperability platform, the introduction of open source software, like e-learning or open desktop, and the master data platform are examples of public administration solutions that may benefit from this cloud initiative.

In short, the services initially offered by the three service models are:

1) *Infrastructure-as-a-Service (IaaS) model*: “the capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications.” [Mell et al. 2009]. The GO-Cloud will start providing computing capacity (CPU, memory and storage), operating systems (OS), database (DBMS) and web servers packaged in three standardized solutions, each one addressing to particular needs. It also provides the basis for supporting the front-end of the GeRALL shared services solutions, like GeRFiP or GeRHuP. The introduction of a virtual desktop solution is also foreseen in a second step;

2) *Platform-as-a-Service (PaaS) model*: “the capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages and tools supported by the provider” [Mell et al. 2009] and middleware applications. Through an on demand based pay per use model, the clients will access to standard platforms to develop and test their own applications. At this stage testing and development solutions will be the first ones to be provided. A repository of software components for customized use like templates, add-ins, add-ons, widgets, and extensibility solutions will be created. However, if not adequately controlled the management and control of these facilities may turn into a complex and costly task. We believe technology still needs some improvement in this domain before a global offer can be made to the Portuguese public administration;

3) *Software-as-a-Service (SaaS) model*: SaaS is seen as applications “accessible from various client devices through a thin client interface such as a web browser” [Mell et al. 2009]. The initial offer will concentrate on: (i) existing SOA applications, like GeSBI; (ii) integration services, like the payment and messaging solutions; and, in a second step, (iii) the introduction of structuring solutions into the public administration, like e-learning.

## 6. Go-Cloud deployment and operational model

The deployment of services in the GO-Cloud is based on service oriented architecture as presented in Figure 3.

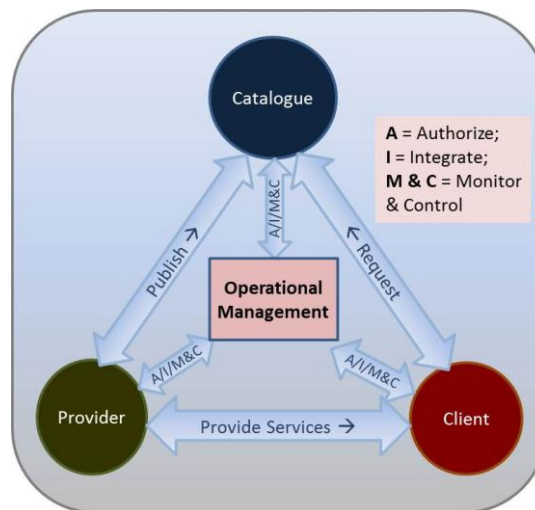


Figure 3 - GO-Cloud Service Oriented Operation Model

This approach, based on web services paradigm, will provide a flexible and service oriented manageable solution.

This model is composed by four major components and their relationship. The central unit, Operational Management, is a management component of the GO-Cloud business management framework that is explained next. It is responsible for the authorization, integration, monitoring and control of cloud resources (level of usage, performance ...), service providers and respective contents, client profiles and related service delivery, and catalogue operational rules and service entries. The Provider and the Client units handle respectively the relationship with service providers and clients. Both components care about contracts, quality of service and service level agreements. The Catalogue unit relates with catalogue operational management.

## 7. GO-Cloud Business Management Framework

The GO-Cloud initiative implementation overlays the double objective of establishing a technological platform that will leverage the shared services adoption spreading among public administration entities, concerning both the already deployed financial and budgetary management solution and the shared human resource management solution, and the provisioning of ICT resources and services in a more flexible and effective way like a shared resource.

The GO-Cloud business management is based on the Shared Services Analysis Model (SSAM) [L. Domingues et al. 2011] as far as the strategic and business layers are concerned, appended with an operational layer for cloud services control and alignment (see Figure 4).

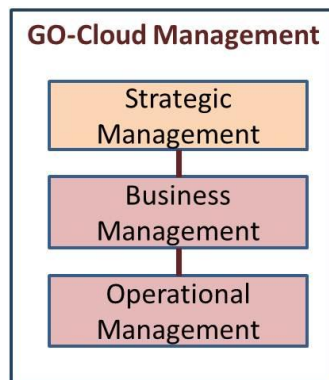


Figure 4 - GO-Cloud Management Framework

The SSAM model [L. Domingues et al. 2011] was developed in order to support shared services implementation management enhancing continuously its performance. To accomplish this propose SSAM model provides a framework to analyse and measure the shared service impact success through two integrated layers:

- **The Strategic Management layer**, is concerned with the overall purpose and scope of delivered products and services. Its activity is framed by the SSAM corporate and business unit strategy layer (see Figure 5), concerning with Go-Cloud continuous market alignment and service governance, as well as GeRAP organisational alignment and intellectual capital management;

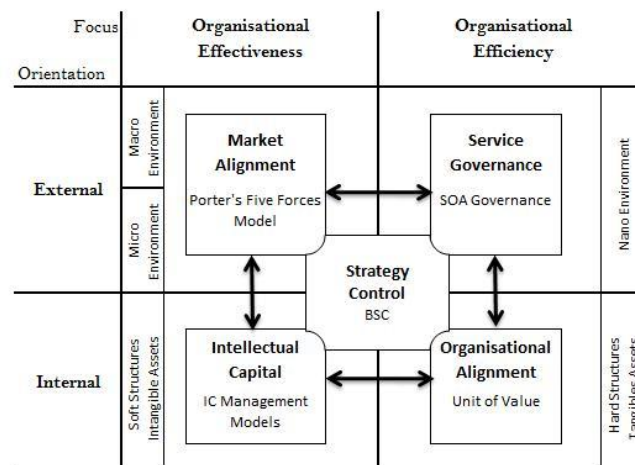


Figure 5 - Corporate and Business Strategy Layer (adapted from SSAM Model)



- **The Business Management layer performs its activity based on the SSAM Operational Strategy layer** (see Figure 6). It is concerned with the way each part of the business is organised in order to deliver the corporate and business-unit level strategic directives, and deals with the implementation of the business unit strategy in which regards resources, processes and people.

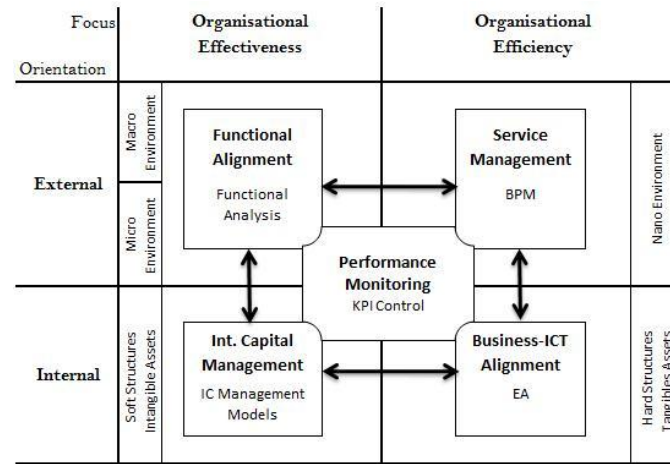


Figure 6 Operational Strategy Layer (adapted from SSAM Model)

As referred before, the main goal of the corporate and business unit strategy layer is to accomplish the strategy definition having as background the environment behaviour addressed by the strategy analysis. On the other hand, the operational strategy layer is mainly focused on the strategy implementation to reach both market needs and company strategic guidelines. The connexion between both layers is performed by a central node related to performance strategy and control based on the balanced scorecard framework [R. S. Kaplan et al. 1996]. The strategy control is defined at the corporate and business unit strategy layer and the performance monitoring, through KPI measurement and control, takes place at the operational strategy layer. Whilst the strategy control influences the strategy implementation, the performance monitoring control impacts the real activity and provides this information to the strategy definition layer through the strategy control.

The **Operational Management layer**, as depicted in the Figure 7, is defined by four pillars resulting from the intersection of the same perspectives followed by the SSAM model, i.e., effectiveness and efficiency versus external and internal analysis. At this level the focus concerns on cloud services implementation and overlays on four pillars: service delivery, catalogue rules, infrastructure and standardization-integration.

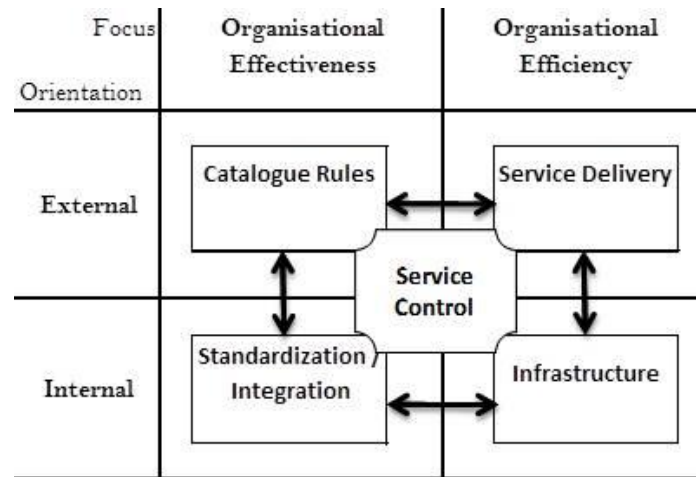


Figure 7 – Operational Layer

The **Catalogue Rules** pillar is responsible for defining main rules to support services providing.

The **Service Delivery** pillar is responsible for deploying services according to clients' contracts assuring that the service is performed in compliance with the established service level agreement, including customization and operational support. Based on ITIL service management processes, the main objective of the Services Delivery component is: (i) to manage the clients' services delivery catalogue, according to both the established policies and signed contracts; (ii) to perform service request management; (iii) to manage incident, problem and change management from the client's perspective; (iv) to deploy templates and allow automation management clients' procedures, integrating their value chains.

It also records and analyses with the operational management unit (see Figure 3) the delivered services with the purpose of controlling and obtaining knowledge about client's consumption behaviour. This is an added-value service that helps to adjust both the offered services and the contracts.

The **Infrastructure** pillar focuses on cloud assets management and operational relationship with providers. Concerning infrastructure management, this pillar, based on a set of ITIL service management processes, comprises several operations: template and automation management; configuration management; incident, problem and change management; image and backup management; IT monitoring and service level management; virtualization management, including scalability; quality control management; capacity planning; products and services development, integration and deployment.

Concerning the operational relationship with GO-Cloud providers this pillar has to: (i) define integrated processes, and develop and deploy the relating interfaces according to the purchase contract established in the business layer; and (ii) spot purchasing involving acquisition of MRO (maintenance, repair and operations) goods not contracted following business guidelines [K. Laudon et al. 2010].

The **Standardization and Integration** pillar is responsible for defining rules to accept and integrate new services.

The **Service Control** unit is responsible for assuring the correct operation and management of the GO-Cloud Operational layer, controlling the activity of the different pillars in order to fulfil the established quality of service levels and assure the strategic alignment with the business layer requirements. The contracts negotiated by the business layer as well as other business

management decisions are translated into the operational layer for implementation. This alignment is supported by the following methods:

- 1) *ITIL service management processes [TSO 2011]*: the outcome of these processes is used to identify key operational metrics;
- 2) *Operational control matrix*: a matrix that encompasses a set of operational metrics.

Based on the ITIL framework, also used by the other layer units, this component is responsible for managing the GO-Cloud operational layer which includes: (i) the control of each operational layer pillar; (ii) incident, problem and change management; (iii) IT service level management; and (iv) capacity and performance management.

The operational control matrix is used to gather a set of layer operational metrics, including those ones provided by operational layer pillars, so that it may have a centralized view of the GO-Cloud health and consequently to provide accurate management information to the upper layer.

## 8. GO-Cloud Governance

The GO-Cloud governance component relates with strategy and the relationship with the public administration and is a CSF for its success.

In order to promote the alignment between the GO-Cloud offered services and the public entities business needs an integrated management framework was designed, integrating GO-Cloud Governance, Management and Services. Figure 8 shows the way they relate.

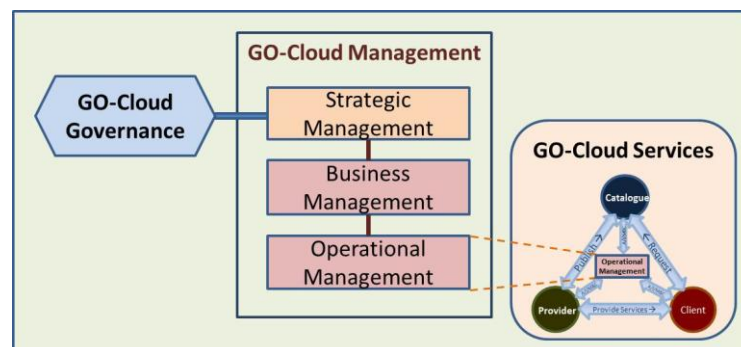


Figure 8 - GO-Cloud Governance and Management framework

## 9. Conclusion

Bearing in mind the three years of experience in implementing shared services within the central public administration we point out the governance and management issues as a critical success factor for the GO-Cloud implementation. The type and the quality of services provided for the cloud are determinant for its acceptance by the public entities. That is the reason why a framework able to provide an open and adaptable solution was defined so that it can cope with future requirements, technological enhancements and market offers.

However, the dynamic behaviour of this type of infrastructures requires both agile management structures and decisions so that alignment can be kept along the time, and efficient metrics and operation services. The presented governance and management framework based on the acquired experience with shared services, aims to provide a suitable answer to these requirements.

## 10. References

- ENISA, "Cloud Computing – Benefits, risks and recommendations for information security". November 2009.
- GeRAP, Portuguese government, "D.-L. 25/2007", 7th of February 2007.
- IGF, Inspeção-Geral de Finanças, "Avaliação aos back-offices da Administração Central do Estado", relatório 1304/2009. Dezembro 2009.
- K. Laudon, J. Laudon. "Management Information Systems". Prentice Hall. 11th Edition. January 9, 2009.
- K. Laudon, Carol Guercio Traver. "E-Commerce 2010". Prentice Hall. 6th Edition. November 21, 2010.
- R. S. Kaplan, David P. Norton. "The Balanced Scorecard: Translating Strategy into Action". Harvard Business Press. September 1, 1996.
- L. Domingues, J. A. Cordeiro Gomes. "Management Model Proposal for Portuguese Public Administration Shared Services". 7th IEEE 2011 World Congress on Services.
- L. Martin. Data Security in the Cloud a Top Concern for Government According to Lockheed Martin Cyber Security Alliance Survey. [Online] April 20, 2010. [http://www.lockheedmartin.com/news/press\\_releases/2010/04-20-cyber-security-alliance-survey.html](http://www.lockheedmartin.com/news/press_releases/2010/04-20-cyber-security-alliance-survey.html).
- L. Tang, J. Dong, Y. Zhao. "Enterprise Cloud Service Architecture". IEEE Computer Society, 2010. 2010 IEEE 3rd International Conference on Cloud Computing. pp. 27-34.
- Mell, Peter e Tim, Grance. The NIST Definition of Cloud Computing. NIST. [Online] 2009. <http://www.nist.gov/itl/cloud/upload/cloud-def-v15.pdf>.
- PRACE, Portuguese council of ministers, "Programa de Reestruturação da Administração Central do Estado", Mars 2006, see [http://www.planotecnologico.pt/document/Modelo\\_PRACE\\_MAR06.pdf](http://www.planotecnologico.pt/document/Modelo_PRACE_MAR06.pdf).
- J. F. Rockart. "A Primer on Critical Success Factors". The Rise of Managerial Computing: The Best of the Center for IS Research. 1981.
- TSO, Best Management Practice. ITIL v3, 2011. See <http://www.best-management-practice.com/officialsite.asp?DI=597910&trackID=002192>.