ICST Transactions
on e-Business
Research Article ICST.ORG

Transformation to Cloud Services Sourcing: Required IT Governance Capabilities

Anton Joha[1,*] and Marijn Janssen[2]

[1]EquaTerra, antonjoha@gmail.com
[2]Delft University of Technology, m.f.w.h.a.janssen@tudelft.nl

Abstract

The sourcing of cloud services is a relatively new type of service delivery model in which an organization gets access to IT services via a cloud service provider that is delivering services over the web to many users on a pay per use or period basis. Even though the importance of IT governance is often underlined, there is limited literature available regarding the required IT governance capabilities that public sector organizations need to have in place to successfully implement and manage a cloud service delivery model. Using an existing governance framework of IT core capabilities as basis, the required cloud computing capabilities are investigated using interviews and studying reports. The analyses helped to identify 16 discriminating capabilities that are essential when effectively implementing and managing cloud services in the public sector. Different factors, including the cloud service and deployment model, the strategic intent underlying cloud sourcing, the degree and complexity of cloud sourcing and the IT governance structure, were found to influence the relevance of cloud capabilities and the relevance might also change over time.

Keywords: Cloud computing, Public sector, IT core capabilities, IT governance, Outsourcing, Public sector, Sourcing.

Received on 14 December 2011; accepted on 05 February 2012; published on 05 September 2012

doi: 10.4108/eb.2012.07-09.e4

1. Introduction

Government agencies are in different stages of development and looking for different ways to improve their service provisioning, while at the same time trying to reduce their costs due to severe budget cuts (Chen, 2003). One way of restructuring IT and business functions is by using cloud computing. A cloud infrastructure consists of application services hosted on a distributed hardware and providing a one point of access for users from anywhere at any time. Clouds can be viewed as a new type of sourcing model in which IT-based services are provided over communication networks to users, enabling for faster implementation of software changes (Bennet et al., 2001) and allowing to get rid of the own installation, control and maintenance of the IT function (Gonçalves & Ballon, 2011). Often, users pay a certain fee for the use of the software or for a certain period that the software will be used. Other forms are possible, but the essence of all forms is that no upfront investments are necessary from the user perspective. Cloud service providers host and provide access to software applications over a network. This type of sourcing model enables the development of a service only once and provides it to many users. Within the public sector there is an opportunity for a similar shift and there are already some notable and visible examples of cloud services, including the use of office applications provided by the cloud model and services to citizens which are hosted in a cloud. In both examples the governmental agencies do not have to develop or maintain the services in-house and they rely on the cloud provider. Cloud services can be provided by organizations within the public sector, but also by private companies residing outside the public sector, in this way providing at least two ways of sourcing.

*Corresponding author. Email: antonjoha@gmail.com

It is often argued that cloud computing has implications for both businesses and management (Olsen, 2006) and cloud computing will change the relationship between buyer and seller (Sääksjärvi et al., 2005). Yet, the specific IT governance capabilities required by public sector organizations to successfully source and manage cloud services have remained unexplored. The goal of this paper is to understand the cloud governance capabilities that are required when introducing and implementing a cloud computing model in the public sector. This paper is structured as follows. In the next section, the background of cloud computing is discussed, including its relationship with outsourcing and the governance framework of IT core capabilities from Feeny and Willcocks (1998) that is used as basis to analyze the interviews and documentation. In section three, the research approach is presented, followed by an overview of the cloud computing activities in the Dutch and US public sector. Section five discusses the findings and conclusions are drawn in section six.

2. Background

2.1. Cloud Computing

There is no agreement about a definition of clouds, though there are some characteristics that are more or less agreed. These are that clouds offer resources on demand (Rosenthal et al., 2010) from which application services can be accessed over a network (Buyya et al., 2009). In most clouds charges are paid per use, but there is no consensus about this characteristic. Rosenthal et al. (2010) provide a set of features of cloud computing. Janssen and Joha (2010) add two additional characteristics based on the idea that a cloud is a distributed system that is presented as one infrastructure that provides services based on service level agreements. These characteristics are:

(1) Resource outsourcing
(2) Utility computing
(3) Large number of (inexpensive) machines
(4) Automated resource management
(5) Virtualization
(6) Parallel computing
(7) Data access control
(8) Service level agreements

A cloud consists of large farms of inexpensive servers which are distributed over several locations. The basic idea of the use of clouds is to shift the responsibility to install and maintain hardware and basic computational services away from the user to the cloud vendor (Rosenthal et al., 2010). The cloud vendor should ensure security, scalability, availability, reliability and data access control mechanisms. In a cloud there is a dedicated pool of hardware and virtualization software that can be used to support a variety of tasks and provide services to the cloud participants. Cloud computing can be categorized into three main service models (Dillon et al., 2010; NIST, 2011c):

- *Cloud Software as a Service (SaaS).* The public sector organization has access to a provider's applications running on a cloud infrastructure. The public sector does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.
- *Cloud Platform as a Service (PaaS).* The public sector organization has the ability to deploy onto the cloud infrastructure customized or acquired applications created using programming languages and tools supported by the provider. The public sector organization does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly application hosting environment configurations.
- *Cloud Infrastructure as a Service (IaaS).* The public sector organization has access to processing, storage, networks, and other fundamental computing resources and is able to deploy and run arbitrary software, which can include operating systems and applications. The public sector organization does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and limited control of select networking components.

The cloud deployment model concerns the specific cloud environment that is used to deliver cloud services to the users. Four deployment models are generally distinguished in the literature (Dillon et al., 2010; Kundra, 2011; NIST, 2011c). A private outsourced cloud is a closed environment for a single organization hosted by a third party, while a private in-house cloud is hosted internally (Kundra, 2011). A public cloud is owned by a SaaS service provider that makes it available to the general public, while a community cloud is shared by several organizations with common policies, requirements, values, and concerns and can either be hosted externally by a third party or in-house **(**Dillon et al., 2010). Hybrid clouds can consist of combinations of the other cloud models. It is postulated that the different forms and deployment models of cloud services will have an influence on the cloud capabilities that are required.

2.2. Clouds and Sourcing

Whereas there is relatively limited research literature about cloud computing, there is a wealth of literature on outsourcing (Gonzalez et al., 2006; Lee et al., 2003). IT outsourcing is about the contracting out of certain IT functions to an external service provider that in return

provides the service for a certain period of time and for a certain amount of money (Willcocks & Kern, 1998). Business Process Outsourcing (BPO) is the situation in which a supplier takes over responsibility for one or more of an organization's business processes (Borman, 2006). Outsourcing arrangements address the relationship between one client having one or more external vendors, and in case a private cloud model is used, this is also the case with sourcing cloud services. In case of a community or public cloud however, the arrangement generally consists of many clients and one cloud vendor. Cloud computing can thus be viewed as a type of sourcing arrangement, in which the cloud service providers can be viewed as a specific type of provider. There are various ways of sourcing like inside or outside the public sector and sourcing requires the use of capabilities for managing sourcing arrangements (Borman, 2006; Feeny & Willcocks, 1998).

2.3. Governance Framework of IT Core Capabilities

Decisions about and around an (out)sourcing transitions are part of a much broader framework called IT governance. IT governance refers to the "patterns of authority for key IT activities" (Sambamurthy & Zmud, 1999, p. 261) and IT governance mechanisms determine how communication, responsibilities and decision-making structures are formalized (Weill & Ross, 2005). Important attributes of IT governance are the roles and responsibilities of the different actors involved (Weill and Ross, 2005) and the related capabilities that are core to the business' future capacity to exploit and govern the demand and supply of IT successfully (Feeny & Willcocks, 1998; Mayer & Salomon, 2006).

Sourcing requires that that the end-user organization has the necessary IT core capabilities to implement and manage the sourcing arrangement. The provider is at an arm's length which requires other capabilities than when having an own IT department. The IT core capability concept is defined by Feeny and Willcocks (1998) and their IT governance framework has been successfully verified in a couple of consecutive articles (Willcocks & Feeny, 2006; Willcocks et al., 2006). Willcocks and Feeny (2006, [p. 49]) define a capability as 'a distinctive set of human resource–based skills, orientations, attitudes, motivations, and behaviors that have the potential, in suitable contexts, to contribute to achieving specific activities and influencing business performance'. Following Willcocks and Feeny (2006) we define a cloud governance capability is a capability to effectively manage and govern the sourcing of cloud services, measurable in terms of IT activities supported, and resulting business performance.

Feeny and Willcocks (1998) view IT capabilities as core to the business's future capacity to exploit IT successfully. Four main areas are defined that a company must successfully address over time: (1) the IT governance area, (2) the technical area, (3) the business area and (4) the supply area. In the governance area, the role of IT within the business is defined, combined with the responsibilities of the IT department, the business departments and the IT service providers in achieving that role, while the technical area is concerned with ensuring that the business has access to the technical capability it needs in order to translate the business requests and requirements into IT specifications (Feeny & Willcocks, 1998). The business area is about demand management and involves defining the business requirements in order to address the need for alignment between business and technology. The supply area, finally, is about managing and monitoring the supplier in order to assure they deliver the required quality of the IT services.

Feeny and Willcocks (1998) initially found nine capabilities that enable a business to consistently address the described four areas in order to exploit IT successfully, now and in the future. In a later article to validate the model, Willcocks et al. (2006) also found a tenth capability, IT project management, though no explicit definition similar to the other capabilities was provided. These ten capabilities and their definitions are depicted in table 1.

Table 1. Governance Framework of IT Core Capabilities (Feeny & Willcocks, 1998; Willcocks et al., 2006)

IT core capabilities	**Definitions (Feeny and Willcocks, 1998)**
1) Leadership	*Integrating IS/IT effort with business purpose and activity*
2) Business systems thinking	*Envisioning the business process that technology makes possible*
3) Relationship building	*Getting the business constructively engaged in IS/IT issues*
4) Architecture planning	*Creating the coherent blueprint for a technical platform that responds to current and future business needs*
5) Making technology work	*Rapidly achieving technical progress, by one means or another.*
6) Informed buying	*Managing the IS/IT sourcing strategy that meets the interests of the business*
7) Contract facilitation	*Ensuring the success of existing contracts for IS/IT services*
8) Contract monitoring	*Protecting the business' contractual position, current and future*
9) Vendor development	*Identifying the potential added value of IS/IT service suppliers*
10) IT Project management	This capability was included in a later paper (Willcocks et al.,

	2006).

These ten capabilities are viewed from the perspective of the end-user organization and not from the supplier perspective. In other research (Feeny et al., 2005; Lacity et al., 2006a; Lacity et al., 2006b) similar kinds of frameworks have been defined with the capabilities relevant to outsourcing service providers.

3. Research Methodology

The research conducted in this paper has an explorative-descriptive nature. Our goal is to develop an understanding of the IT governance capabilities required for public sector organizations that want to successfully implement and manage cloud services. This research takes the governance framework of IT core capabilities by Feeny and Willcocks (1998) as a starting point, extending and refining it for cloud computing. This model is useful as it finds its roots in outsourcing relationships and cloud computing can be viewed as a type of sourcing arrangement, in which the cloud providers can be viewed as a specific type of outsourcing provider. Exploratory research was chosen due to the need to investigate and explore the IT governance capabilities required by public sector organizations for cloud computing arrangements. Interviews were conducted within the Dutch government and these were complemented by studying international case study reports and documents. Interviews allowed us to explore and in-depth discuss the concept of cloud computing, in this way creating a better understanding of the possible challenges and the required capabilities when adopting and managing cloud services in the public sector. Thirteen interviews were conducted using open-ended questions, informed in many ways by our understanding of cloud services and outsourcing as presented in the background of this paper. The interviews lasted between one and two and a half hours and the interviewees included Dutch IT-managers, outsourcing specialists, outsourcing and cloud decision-makers and IT-experts from a variety of public organizations, including the tax authority, social security agency, Ministry of the Interior and Kingdom Relations, municipality association and two municipalities. In this way, a broad range of organizations and views were covered. Interviewees covered persons in organizations that were already using cloud services as well as those who are considering the use of cloud computing or did not decide to use it.

4. Clouds Sourcing in the Public Sector

The Dutch cloud strategy was driven by the cloud strategies in the US. Both the Dutch and the US public sector consist of many organizations that have IT environments that can be characterized as difficult to manage, heterogeneous, with duplicative systems with low asset utilization, negatively impacting its ability to serve its citizens. There are several big public organizations having large data centers and many small organizations that find it hard to manage their IT services and resources. The US government developed a decision framework that was created to support agencies in migrating towards cloud services such as cloud-based SaaS, PaaS and IaaS. The revenue model proposed was based on the idea that users will only pay for the IT resources they consume, and would be able to increase or decrease their usage to match their requirements and potential budget constraints. Following the publication of this strategy, each agency was required to re-evaluate its technology sourcing strategy to assess the use and implementation of cloud-based technology and application solutions as part of the budget process (Kundra, 2011). In the Netherlands it was recently decided to create a public cloud infrastructure. The rationale is based on the reduction of the 61 data centres and the lowering of energy consumption which accounts for 15 million annually (Hillenaar, 2010).

5. Analysis and Discussion

5.1. Cloud Governance Capabilities

Feeny and Willcocks' (1998) governance framework of IT core capabilities was used to identify the capabilities that are core for the implementation of a cloud computing service delivery model for the public sector. Table 2 shows each of the 10 IT core capabilities and how they relate to the 16 identified cloud governance capabilities that are required when sourcing and managing cloud services. The table also shows the typical role(s) involved in executing each cloud capability, as this was an important indicator to identify the discriminating cloud capabilities. The relationship between a role and an individual can be clarified as follows:

- One role can be fulfilled by one or more individuals;
- One individual can fulfill one or more roles.

Table 2. Identified IT Governance Capabilities for Sourcing Cloud Services

IT core capabilities as defined by Feeny and Willcocks (1998)	**Redefined and extended IT governance capabilities for sourcing cloud services**	**Clarification of the IT governance capabilities for sourcing cloud services**	**Typical role(s) involved in executing each cloud capability**
1) Leadership	1) Cloud Leadership	Defining the overall federal IT governance and strategy in terms of the organizational structures, the processes and the staffing relevant to the cloud services, in order to address all the main activities in the business, technical and supply areas and to manage all potential (inter)dependencies between these areas.	Federal CIO, agency executive
2) Business systems thinking	2) Cloud Business Strategy and Policy	Defining the decentralized business strategy and the translation of that strategy to a cloud strategy, where choices have to be made about the role and the priority of cloud services within the organization, including the make or buy decision about sourcing cloud services.	Business unit CIO/manager, Head of IT
3) Relationship building	3) Demand Management	Defining business functionality and its dependencies, including the translation to IT/cloud specifications, demand forecasting and interfacing with the end users.	Information manager
	4) Relationship Management	Providing a single point of contact through which the business organization can ensure that problems and conflicts are resolved fairly and promptly, within a framework of agreements and relationships.	Relationship manager
4) Architecture planning	5) Architectural Design and Standards	Creating the coherent blueprint for a technical cloud platform that responds to current and future business needs and maintaining the technical consistency and standards between cloud information systems.	Infrastructure architect
	6) Data Security Management	Ensuring data security, privacy, compliance, portability and interoperability.	Data architect, cloud security specialist
	7) Application Lifecycle Management	Responsible for software design, coding, testing and configuration of customized cloud business applications, but also for cloud application maintenance and application upgrades	Cloud application developer
5) Making technology work	8) IT Network Management	Given that the Internet and intranet are the main ways to access cloud application services, the IT network management capability needs to ensure that potential network problems can be rapidly fixed.	Network specialist, infrastructure manager
6) Informed buying	9) IT/Cloud Procurement	Tracking cloud market developments and suppliers and leading the selection process for cloud services including negotiating about procurement terms and conditions with suppliers.	IT/cloud procurement officer
	10) Risk and Compliance Management	Monitoring and auditing potential risk/compliance issues involved in sourcing cloud services.	Risk officer, auditor
	11) Legal Expertise	Providing support when entering into (new) agreements with cloud service providers and making changes to existing contracts, including handling all legal issues related to clouds.	Legal advisor
7) Contract facilitation	12) User Support	Providing support to users by means of training and by a (self) service desk.	Service desk employee
8) Contract monitoring	13) Contract Management	Ensuring contractual compliance by the cloud providers on strategic and tactical level and managing any required contract modifications, taking into account all the relevant aspects including financial, legal, technical and business dimensions.	Contract manager
	14) Service Management	Managing the performance of the service delivery on tactical and operational level as specified in the contractual performance metrics, including performance management and maintenance of the cloud service catalogue.	Service manager
	15) Financial Control	Tracking, monitoring and reporting on the IT budget and ensuring that the cloud services meet the committed and predefined financial goals.	Financial controller
9) Vendor		The ‘vendor development’ capability was not distinguished as a	

development		specific capability or role. Creating added value happens at each level and role of the supply area and this specific capability can be incorporated within all the other capabilities.	
10) IT Project Management	16) IT Project and Portfolio Management	Managing a project or a portfolio of multiple ongoing inter-dependent cloud projects that are executed internally and/or by cloud providers.	Project / program manager

Five capabilities in Feeny and Willcocks' framework could almost be individually translated to the cloud domain, though they needed some refinement, both in terms of the terminology used for the capability as well as for the definitions. In four instances, the capabilities defined by Feeny and Willcocks (1998) have been split into 2 or more different capabilities because of the special importance of these capabilities for cloud computing and because of the distinct and different nature of these capabilities in terms of roles. One capability in Feeny and Willcocks' framework, vendor development, was not distinguished as a specific capability or role. This capability is meant to ensure that added value is created by IT outsourcing, but creating added value happens at each level and role of the supply area and this specific capability can therefore be incorporated within all the other individual capabilities within the supply area. In the part hereafter the capabilities are discussed in more detail.

Cloud Leadership

Cloud leadership is about defining the overall federal IT/cloud governance and strategy in terms of the organizational structures, the processes and the staffing, in order to address all the main activities in the business, technical and supply areas and to manage all potential (inter)dependencies between these areas. It also includes creating organization-wide support and strategic stakeholder management for implementing cloud services. Interviewees indicated that the choice for cloud computing is a decision that has a long-term and strategic impact, requiring significant organizational changes in order to adopt and manage this new service delivery model. The US federal government created a 25-point federal IT reform plan to address their new IT strategy, in which cloud computing was an important element (Kundra, 2010).

Cloud Business Strategy and Policy

This capability is concerned with defining, integrating and aligning the business objectives with IT/cloud capability. The overall business strategy from all of the decentralized governmental agencies has to be translated to a cloud strategy, resulting in an information policy, which takes into account all the requirements and potential (im)possibilities of the cloud solution. This also includes defining the sourcing strategy in terms of the decision to outsource or not and all the relevant strategic choices related to this decision including which cloud deployment models can be used. Although clouds can be outsourced to a service provider, clouds can also be operated as internal arrangements within the government. In such a construction the internal IT department will function as the cloud service provider. Interviewed governmental representatives mentioned that this would enable governments to better keep control over their privacy sensitive data, avoid potential security problems, ensure authorization, identification and encryption, and to avoid legislation and regulation risks by outsourcing this to a third party and nevertheless gain advantages of this development.

Agencies could bypass the federal or internal IT department to acquire their own cloud services, which could create difficulties in data integration or service interoperability in the future within the public sector and therefore overall policy standards and guidelines need to be defined. The policy needs to be followed by agencies to ensure that the agencies comply to regulatory or legal requirements, to enforce organization-wide consistency and to make sure that the agencies have guidelines in case they want to use cloud services. As such, the US government published a federal cloud computing strategy, providing a decision framework to support agencies in migrating towards services such as cloud-based SaaS, PaaS and IaaS (Kundra, 2011).

Demand Management

The demand management capability facilitates the dialogue between the business and the IT department regarding cloud services and is responsible for defining the functional requirements with regard to the cloud solution. The defined cloud policy has to be translated into cloud functionality and the underlying specifications and service levels with regard to the cloud services have to be defined. This capability also includes demand forecast for the expected consumption and use of cloud services by the agencies, ensuring alignment with corporate IT, controlling the decentralized cloud budget and monitoring local cloud SLAs. Agencies could have the possibility to directly buy services from the cloud provider by means of a service catalogue, which is a document listing the portfolio of possible cloud services that the agencies can buy from the cloud service provider(s) supported by the cloud outsourcing contract.

Relationship Management

This capability involves managing the requirements and problems within the business units with regard to the cloud services. Relationship management provides a single point of contact through which the business organization can ensure that problems and conflicts are resolved fairly and promptly, within a framework of agreements and relationships. It involves also handling requests from decentralized entities for action on issues that range from minor questions to very significant crises,

being the focal point of contact for business managers, facilitating people relationships and devising processes for conflict resolutions regarding the cloud delivery model.

Architectural Design and Standards

Through insight into technology, cloud service providers and the requirements from agencies, the architectural design and standards capability is about the development of the vision of an appropriate technical cloud platform. Without such planning, the organization could end up with independent systems that might result in redundancy, gaps between systems or the inability to integrate cloud systems. Cloud standards need to be determined with regard to the technical platforms, e.g. networks, protocols, resilience. Questions about standardization, security of the architecture, the necessary flexibility and the integration with other components need to be addressed, but also the implications for the people using the technology. In the US federal government a lot of attention is paid to standards (NIST, 2011b) and there is a central group involved with standards management responsible for establishing a framework and roadmap to define standards facilitating interoperability, portability and security of cloud services.

Data Security Management

The data security management capability involves setting enterprise level data requirements regarding security, privacy and compliancy and enforcing policies for protecting sensitive corporate and customer data from being shared, including managing all forms of virus prevention and detection relative to public cloud services
This also comprises the development of a framework for sharing user identities and providing user access to sensitive data, including conditions under which service providers, third parties and government agencies may have access to the company's data. The framework should include authentication, authorization and use of physical devices like digital signatures, encryption, social barriers, and monitoring by humans and automated systems. The framework should be audited and updated regularly to address changing technology and service delivery mechanisms. In the federal US government a central security department was set up in order to identify, aggregate, and disseminate security, privacy and compliance issues, solutions and processes that could impact the adoption and implementation of cloud services.

Application Lifecycle Management

Application lifecycle management is responsible for software design, coding, testing and configuration of customized business applications, but also for application maintenance and application upgrades. Activities include monitoring emerging cloud technologies and leading the investigation and adaptation of new cloud application technology, documenting the existing cloud application architecture portfolio, setting formal policies and processes to integrate cloud applications; defining processes and criteria for granting exceptions to the cloud applications standards and defining architecture components and interfaces based on application architectural standards with regard to cloud computing.

IT Network Management

In cloud computing, it is essential that the network capacity is meeting the required standards as the Internet and intranet are the main ways to access cloud application services. IT network management is about ensuring the quality of the network and local or remote servers. The cloud infrastructure should have the necessary capacity and processing power at all times. This network capability could be outsourced, but it was suggested by interviewees that it is important that potential network problems can be rapidly fixed and to retain parts of this capability in-house. The main risk is that increasingly less operational technology knowledge seems to be necessary in cloud arrangements, while the dependency on the service providers is increasing. The network dependency is also recognized as such by the National Institute of Standards and Technology (NIST, 2011a) recommending that the traditional IT skills required to manage devices that access the private cloud need to be retained, also for managing special hardware or system requirements and unique security needs for special projects.

IT/Cloud Procurement

IT/Cloud procurement is responsible for analyzing the cloud service providers and leading the procurement process for the selection of a cloud provider till the moment the contract has been signed. This includes managing the Request for Proposal (RFP) process, which includes the collection and verification of equipment and component requirements and SLA specifications, development of the RFP, evaluation of the responses and giving recommendations for supplier selection to the agencies.
This also includes the responsibility for assuring that the cloud procurement is completed within the predefined timeframe and meets the identified cost objectives as well as continuously analyzing the external cloud services market.

Risk and Compliance Management

This capability needs to ensure that potential regulatory and compliance risks are identified and also needs to continuously confirm that the assurance methods adopted by service providers are evolving to include, in addition to SAS 70, the new Service Organization Controls (SOC) reporting model and other cloud security certifications.
The cloud infrastructure should be secure and reliable. Although contractually this might be arranged, public organizations do not want to be confronted with problems. Therefore regular audits, either internally by a separate department, or externally, are necessary to determine if the cloud vendor's infrastructure and support is compliant to the contract. These audits need to be part of risk and

compliance management. Security policies, but also backup, recovery and contingency procedures and plans should be regularly evaluated to account for potential cloud provider failure. Interviewees were suggesting that clear agreements about data ownership need to be made including what will happen in case a SaaS provider goes bankrupt, is taken over by another company, or is changing its strategic orientation and vision.
The interviewees were very reluctant to move to a cloud model on a large scale without any assurances, because of the dependency on the cloud provider, and as part of the risk process, a careful migration strategy was therefore suggested. The interviewees argued that applications and information that are of particular importance must initially be retained in-house and run on the own IT system, but can be maintained by the cloud providers. In case of dissatisfaction with what comes as part of the package with the cloud provider, those applications can immediately be taken over by the own staff. This means less risks, but higher retained software costs for the client than may have been initially assumed, and those costs should be understood and be part of the initial business case justifying the use of cloud services.

Legal Expertise

Legal expertise provides support when entering into (new) agreements with cloud service providers and making changes to existing contracts. Out of the interviews, it became clear that the location of storage is an issue, as Dutch governments often require that data will be stored within the Netherlands to ensure that the Dutch law will be in effect to the SaaS providers. It is likely that new agencies or authorities are required to verify and control that data does not cross national boundaries and that licenses are legal. In general the contract needs to take into account issues regarding data protection and regulatory compliance, intellectual property concerns and contingency in the event of business discontinuity caused by the service provider. Also the risks of non-performance and potential exit scenarios need to be contractually defined.

User Support

Interviewees indicated that as cloud services are based on a hosted delivery model, users may find they do not have access to the same level of service and support they would get from their internal IT group or would get in an outsourcing arrangement. As such a (self) service desk needs to be in place for any user support. Supporting and training users on new functionality delivered via the more frequent upgrades enabled by the cloud model requires skilled resources, but not all cloud providers will offer the level of support required to meet end-user needs, especially during initial implementation efforts. As a result, public sector organizations must account, plan and budget for all required support requirements.

Contract Management

Contract management is about ensuring contractual compliance by the cloud provider(s) on strategic and tactical level and managing any required contract modifications, taking into account all the relevant aspects including financial, legal, technical and business dimensions. This includes contract administration, monitoring compliance with terms and conditions, review and revision of contract changes, supplier negotiation and contract interpretation for dispute resolution. Long term sustainability is a key issue, as the bankruptcy or other problems of the cloud vendor could jeopardize certain business operations. Data might simply not be available anymore in specific circumstances.
The interviewees considered good contracts to be essential, as this is an important instrument to avoid the risks and accomplish the benefits of cloud computing. Contracts are more complicated as it should be flexible and demands instant scaling up based on pay per use on the one hand, whereas on the other hand long-term sustainability, software access and information storage requirements need to be met. These short term and long term interests might be conflicting, as the cloud provider might require some kind of payment of longer term commitments are part of the contract. Effective contract monitoring means holding suppliers to account on both existing service contracts and the developing performance standards of the services market. This includes developing service level measures and service level reports, specifying escalation procedures and cash penalties for non-performance (Kern and Willcocks, 2001).

Service Management

The service management capability involves managing the performance of the service delivery on a tactical and operational level as specified in the contractual performance metrics, including performance management and maintenance of the service catalogue, to ensure that performance targets continue to be met, users remain satisfied, the expected service levels continue to be achieved and the services continue to be performed and delivered in the expected manner. This includes monitoring, reviewing, managing, changing and reporting on all cloud service levels. The cloud provider is normally able to retrieve information regarding SLA compliance, usage levels, account activity, etc. Further activities include, but are not limited to, ensuring that the cloud performance review system and the SLA metrics are maintained to be relevant to the outsourcing contract, applying service level penalties if the cloud supplier performs below the service credit threshold and approving change requirements.

Financial Control

Financial control is about tracking, monitoring and reporting on the IT/cloud budget and ensuring that the outsourced services meet the committed and predefined financial goals. Relevant activities include directing and coordinating the organization's financial IT planning and IT/cloud budget management functions, recommending

benchmarks for measuring the financial and operating performance of the cloud supplier, monitoring the overall cost of the cloud contract, preparing financial analysis for contract negotiations with the cloud supplier, and coordinating with the contract administration for payment procedures and budget procedures related to the delivered cloud services.

IT Project and Portfolio Management

IT project management is the application of knowledge, skills, tools, and techniques to plan and execute IT project activities that meet the predefined objectives in terms of planning, cost and quality (Project Management Institute, 2000). Especially for cloud computing services, the transition and migration strategy and activities have been recognized as very important by the interviewees. This capability includes identifying and planning project activities, minimizing risk and managing the project, the resources and team members. When implementing cloud services also the (inter)dependencies with other IT/cloud projects need to be taken into account, managing multiple projects as a portfolio. This capability was initially not included in Feeny and Willcocks' IT capability framework as they considered project management not as a specific IT core capability but as an organizational one. When verifying their model however, they also found this capability to be distinctive to the IT function (Willcocks et al., 2006).

Based on the analysis in the former section, Feeny and Willcocks' capability model could be refined and extended for cloud computing. In Figure 1, the sixteen distinguished cloud governance capabilities have been plotted within the governance, business, technical and supply area.

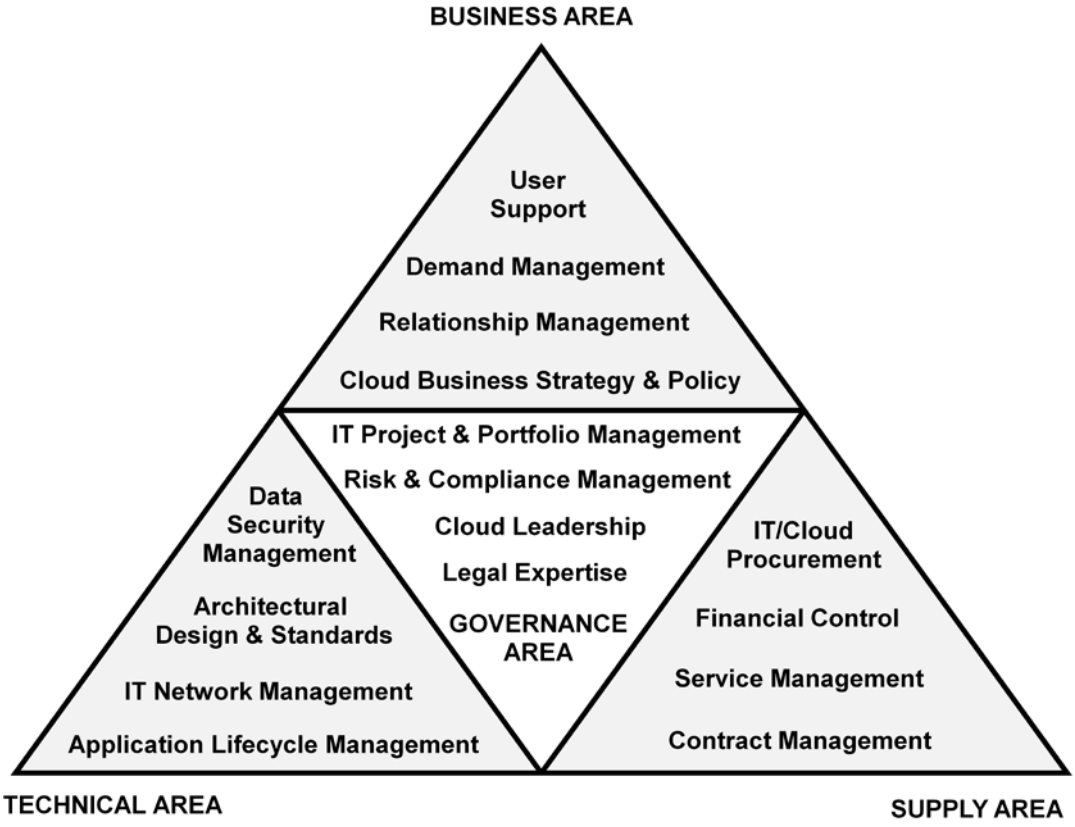

Figure 1. Cloud Governance Capability Model (based on Feeny & Willcocks, 1998; Willcocks et al., 2006)

Several interviewees mentioned that uncoordinated adoption and not having the appropriate capabilities in place could undercut the financial benefits of cloud computing, and severely increase the risks. They indicated the need to first find out which capabilities are required and ensuring that investments can be made and organizational structures and routines are in place before the cloud model can be used on a large scale. By developing and implementing the required capabilities first and experiment on a small scale, the intricacies and expertise needed could be discovered.

5.2. Relevance of the Cloud Capabilities

Determining the relevance of the different capabilities is important in order to determine which and how many individuals can fulfill the role involved in executing the

respective capability. When the relevance of a certain capability increases, it implies that either a higher quality of the individual fulfilling that capability is required, or that more individuals are necessary to fulfill that specific capability. When the relevance of a capability decreases, it implies that this capability might be integrated with other related capabilities so that one individual can fulfill a role that covers multiple capabilities. There are different factors identified that influence the relevance of the capabilities in some way or another and these will be discussed in the following paragraphs.

Cloud Service and Deployment Model

The capabilities in the governance area were found to be relevant for all cloud service models. Leadership is required for all cloud implementations, and so is the IT project and portfolio management capability to successfully implement the cloud solution taking into account all the (inter)dependencies. Legal expertise and risk and compliance management need to be in place in order to ensure that as many legal and compliancy risks are mitigated and minimized. The capabilities within the technical domain are more important in IaaS and PaaS arrangements than in SaaS arrangements, as the cloud provider will be having more technical responsibilities in SaaS arrangements. The importance of the capabilities within the supply area will therefore however increase in SaaS arrangements because of the increased dependency on the service provider. Also the capabilities within the business area are more important in SaaS arrangements given the critical business nature of the applications.

There are also differences between the control and capabilities required for private and public clouds, as in the latter case there will be an increased emphasis on the capabilities within the supply area given the decreased control over a public cloud.

Strategic Intent Underlying Cloud Sourcing

The strategic intent underlying cloud sourcing refers to the benefits that are sought to be achieved by introducing and implementing cloud services. In the US federal government all participating agencies can prioritize one or more different strategic intents and according to their individual requirements, an appropriate cloud solution can be provided. In case the main focus is on cost reductions and/or cost savings, the importance of the supply management capabilities such as financial control and contract management will increase to ensure that costs will be properly managed and the expected cost savings and reductions will be achieved.

In case the main focus is to improve the services to the business by delivering more precisely on changing business requirements, the importance of the capabilities within the business area will increase, as the functional requirements from a business perspective will have to be defined and translated to an appropriate cloud solution.

Degree and Complexity of Cloud Sourcing

The need to manage an outsourcing arrangement increases proportionally with the degree of outsourcing in terms of the size of the outsourcing deal(s) (Barthélemy, 2001; Kern & Willcocks, 2001). The more clouds have been outsourced to multiple vendors and the higher the contract value, the higher the costs will be to transition the cloud activities to a new supplier or to insource the activities again. This implies that more control is needed, not only from contract management, service management and financial control, but also from the capabilities in the governance area to mitigate the risks as much as possible.

When the variety and number of cloud projects increase, so will the complexity of the relationship with the cloud vendor(s). An increase of complexity might well result in an increase of the number of hierarchical levels and requires further standardization of procedures (Kern & Willcocks, 2001). The governance capabilities become more important, because the organizational structures, processes and procedures need to become formalized and standardized as much as possible to improve the coordination. The technical area will also rise in relevance as the responsibility to provide the expertise for the technical standardization and integration of the different cloud activities is within this area. It was suggested that also in case of only in-house clouds, all 16 capabilities are required, as public organizations will increasingly have to develop and professionalize their own internal organization in such as way as if they would interact with the external market.

IT Governance Structure

An important organizational factor is whether the IT governance structure is centralized, decentralized or federated, which was also found by Earl et al. (1996) and Sambamurthy and Zmud (1999). In case of a centralized IT governance structure, the capabilities in the technical and supply area become more important as there will typically be a focus on increasing standardization and efficiency. In case there is a decentralized IT governance structure, the capabilities in the business area will become more important, as the IT function will be mainly controlled by the decentralized business entities which are responsible for defining the cloud strategy and their specific cloud requirements. In a federated IT governance structure the control over the IT function is divided between central and decentral units, increasing the need for strong leadership and coordination (Hodgkinson, 1996). As such, the capabilities in the governance area will increase in importance.

5.3. Differences with regular IT Outsourcing

There are several differences between the capabilities required for regular IT outsourcing services compared to those relevant for cloud sourcing. Given the dependency on the service provider and that there are other risks involved than in normal outsourcing arrangements, risk and compliancy management and legal expertise are

important capabilities for cloud arrangements. These risks, including security and privacy risks, also need to be taken into consideration in the technical dimension with additional capabilities such as data security management and application lifecycle management. Some interviewees indicated that cloud computing is changing the nature of the organization, providing more decentralized power to the business users and therefore also making the business capabilities more important than in regular outsourcing arrangements. Because of this shift, it was also suggested that certain capabilities within the supply domain, e.g. contract and service management, though relevant, were less demanding roles than within regular outsourcing arrangements. Another important remark is that at some point the cloud market will become more mature and standardized in terms of legal contracts, security and compliance standards and that certain capabilities will become less relevant over time when industry standards and best practices become available.

6. Conclusion

A cloud governance capability can be defined as a capability to effectively manage and govern the sourcing of cloud services, measurable in terms of IT activities supported, and resulting business performance. Different core capabilities were required to manage the internal cloud computing demand management process and the external cloud service provider(s). These capabilities can be used by strategists and policy-makers to stimulate the developments of capabilities needed by organizations to manage their cloud providers.

Even though the importance of IT governance is often underlined, there is very limited research literature available regarding the required IT governance capabilities that public sector organizations need to have into place to successfully implement a cloud service delivery model. This paper fills that gap by identifying the IT governance capabilities that are required when introducing and implementing a cloud service delivery model. Using the governance framework of IT core capabilities by Feeny and Willcocks (1998), 16 core cloud capabilities are identified. These are:

1) Cloud Leadership
2) Cloud Business Strategy and Policy
3) Demand Management
4) Relationship Management
5) Architectural Design and Standards
6) Data Security Management
7) Application Lifecycle Management
8) IT Network Management
9) IT/Cloud Procurement
10) Risk and Compliance Management
11) Legal Expertise
12) User Support
13) Contract Management
14) Financial Control
15) Service Management
16) IT Project and Portfolio Management

Several interviewees indicated that uncoordinated adoption of cloud computing and not having the required capabilities in place could increase the risks and undercut the financial benefits of cloud computing. As such, governments need to adopt these capabilities when transforming their operations to cloud computing.

Feeny and Willcocks' governance framework of IT core capabilities framework was found to be appropriate to customize it for cloud computing. Therefore we argue that in general this framework will be useful as a starting point, but further customization and detailing might be necessary to adopt it for a specific domain.

The analyses show that that there are differences between the capabilities required for cloud services compared to those required for regular IT outsourcing services relating to the fact that there are more uncertainties and risks involved in cloud computing that need to be properly mitigated. Moreover, it was found that different factors influence the importance of each of the cloud capabilities, including the cloud service and deployment model, the strategic intent underlying cloud sourcing, the degree and complexity of cloud sourcing and the IT governance structure. The importance of the capabilities can also change over time.

As the market for cloud services is still in its infancy and is expected to significantly evolve over the coming years, there are no best practices yet providing a definitive list of required governance capabilities to manage cloud arrangements and as such this model will need further verification. Further quantitative research into the factors influencing the relevance and quality of these capabilities would also be of interest, including the question if, and to what extent, the identified cloud governance capabilities are different for private sector organizations.

References

Barthélemy, Jérôme (2001). The Hidden Costs of IT Outsourcing. *Sloan Management Review*, 42(3), 60-69.

Bennet, K. H., Munro, M., Gold, N., Layzell, P. J., Budgen, D. & Brereton, O. P. (2001). *An Architectural Model for Service-Based Software with Ultra-Rapid Evolution.* Paper presented at the Proceedings of the 17th IEEE International Conference on Software Maintenance (ICSM'01) Florence.

Borman, M. (2006). Applying multiple perspectives to the BPO decision: a case study of call centres in Australia. *Journal of Information Technology, 21*(2), 99-115.

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J. & Brandi, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems, 25*(6), 599-616.

Chen, H. (2003). Digital Government: technologies and practices. *Decision Support Systems, 34*(3), 223-227.

Dillon, T., Wu, C. & Chang, E. (2010). *Cloud computing: issues and challenges.* Paper presented at the 24th IEEE International Conference on Advanced Information

Networking and Applications. Retrieved from http://xml.ice.ntnu.edu.tw/JSPWiki/attach/Focusardi/Cloud%20Computing%20Issues%20and%20Challenges.pdf

Earl, Michael J., Edwards, Brian & Feeny, David F. (1996). Configuring the IS function in Complex Organizations. In: Earl, Michael J., Information Management: the Organizational Dimension, *Oxford University Press.*

Feeny, D. F., Lacity, M. & Willcocks, L. P. (2005). Taking the Measure of Outsourcing Providers: Successful outsourcing of back office business functions requires knowing not only your company's needs but also the 12 core capabilities that are key criteria for screening suppliers. *Sloan Management Review*, *46*(3), 41-49.

Feeny, D. & Willcocks, L. P. (1998). Core IS Capabilities fo Exploiting Information Technology. *Sloan Management Review*, *39*(3), 9-21.

Gonçalves, V. & Ballon, P. (2011). Adding value to the network: Mobile operators' experiments with Software-as-a-Service and Platform-as-a-Service models. *Telematics and Informatics*, *28*(1), 12-21.

Gonzalez, R., Gasco, J. & Llopis, J. (2006). Information systems outsourcing: A literature analysis. *Information & Management*, *43*, 821-834.

Hillenaar, M. (2010). Rationalisering en groen om ICT kosten te besparen. Retrieved 11 November, 2011, from http://www.ratioconsultants.nl/?p=979

Hodgkinson, Stephen L. (1996). The Role of the Corporate IT Function in the Federal IT Organization. In: Earl, Michael J., Information Management: the Organizational Dimension, *Oxford University Press*.

Janssen, M. & Joha, A. (2010). *Connecting cloud infrastructures with shared services.* Paper presented at the Proceedings of the 11th Annual International Digital Government Research Conference on Public Administration Online: Challenges and Opportunities, Pueblo, Mexico.

Kern, T. & Willcocks L.P. (2001). The Relationship Advantage: Information Technologies, Sourcing, and Management, *Oxford University Press.*

Kundra, V. (2010). *25 Point Implementation Plan to Reform Federal Information Technology Management*.

Kundra, V. (2011). *Federal Cloud Computing Strategy*.

Lacity, M., Feeny, D. & Willcocks, L. P. (2006b). *The twelve supplier capabilities: part II.* Arlington, MA., USA: Cutter Consortium.

Lacity, M., Willcocks, L. P. & Feeny, D. (2006a). *The twelve supplier capabilities: part I.* Arlington, MA., USA: Cutter Consortium.

Lee, J. N., Huynh, M. Q., Kwok, R. C. W. & Pi, S. M. (2003). IT Outsourcing Evolution. Past, Present and Future. *Communications of the ACM*, *46*(5), 84-89.

Mayer, K. J. & Salomon, R. (2006). Capabilities, contractual hazards, and governance: Integrating resource-based and transaction cost perspectives. *Academy of Management Journal*, *49*(5), 942-959.

NIST. (2011a). Draft Cloud Computing Synopsis and Recommendations. Retrieved 5 November, 2011, from http://csrc.nist.gov/publications/drafts/800-146/Draft-NIST-SP800-146.pdf

NIST. (2011b). NIST Cloud Computing Standards Roadmap. Retrieved 5 November, 2011, from http://collaborate.nist.gov/twiki-cloud-computing/pub/CloudComputing/StandardsRoadmap/NIST_SP_500-291_Jul5A.pdf

NIST. (2011c). The NIST Definition of Cloud Computing. Retrieved 5 November, 2011, from http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

Olsen, E. R. (2006). *Transitioning to Software as a Service: Realigning Software Engineering Practices with the New Business Model*. Paper presented at the IEEE International Conference onService Operations and Logistics, and Informatics, 2006 (SOLI '06).

Project Management Institute (2000). *A Guide to the Project Management Body of Knowledge (PMBOK guide)*. Project Management Institute, USA.

Rosenthal, A., Mork, P., Li, M. H., Stanford, J., Koester, D. & Reynolds, P. (2010). Cloud computing: A new business paradigm for biomedical information sharing. *Journal of Biomedical Informatics*, *43*(21), 342-353.

Sääksjärvi, M., Lassila, A. & Nordström, H. (2005). *Evaluating the software as a service business model: From CPU time-sharing to online innovation sharing*. Paper presented at the IADIS International Conference e-Society 2005.

Sambamurthy, V. & Zmud, R. W. (1999). Arrangements for Information Technology Governance: A Theory of Multiple Contingencies. *MIS Quarterly*, *23*(2), 261-290.

Weill, P. & Ross, J. W. (2005). A matrixed approach to designing IT governance. *MIT Sloan Management Review*, *46*(2), 26-34.

Willcocks, L. P. & Feeny, D. (2006). IT outsourcing and core IS capabilities: challenges and lessons at Dupont. *Information Systems Management*, *23* (1), 49-56.

Willcocks, L. P. Feeny, D., & Olson, N. (2006). Implementing core IS capabilities: Feeny-Willcocks IT governance and management framework revisited. *European Management Journal*, *24* (1), 28-37.

Willcocks, L. P. & Kern, T. (1998). IT Outsourcing as Strategic Partnering: The case of the UK Inland Revenue. *European Journal of Information Systems*, *7*(1), 29-45.