# N.J. Division of Revenue and Enterprise Services


PLANNING FOR CLOUD COMPUTING PROCUREMENTS: FRAMEWORK AND ELEMENTS

June 25, 2019

**Abstract**

This research paper, developed by James Fruscione, Director of the New Jersey Division of Revenue and Enterprise Services, covers the core considerations associated with planning for cloud computing procurements. Drawing upon information presented in professional and academic literature, Mr. Fruscione delineates a prescriptive conceptual framework that sets forth basic cloud computing procurement planning elements. These elements include cloud deployment/service models, service levels, pricing, security, operations, and contract governance/management. The paper also highlights how the planning framework serves as the starting point and foundation for the entire cloud computing engagement by generating inputs and guidance for various phases of the procurement life-cycle. Organizations across sectors -- public, private and non-profit, may find the paper helpful. The paper should not be construed as a policy directive from the State of New Jersey. Additionally, the paper does not endorse any specific commercial solutions or platforms.

*Key words*: cloud computing, procurement planning, contracting, information technology

Planning for Cloud Computing Procurements, Framework and Elements

## Introduction

Cloud computing is rapidly becoming a ubiquitous model for information processing and management. The National Institute of Standards and Technology (2013) defines cloud computing as network-based access to standardized, pooled (virtualized) and configurable computing resources. These resources encompass computer memory, processors, data storage, network bandwidth and software of all kinds. Cloud computing enables organizations to access services and resources as needed (on-demand) via various networked machinery such as desktop and laptop computers, and mobile devices like smart phones and tablets (Laudon & Laudon, 2014).

While some may opt to develop their own in-house cloud computing programs, it is common for institutions to use outside cloud computing contractors (How Cloud Computing is Influencing Procurement, n.d.). These third party arrangements offer a number of important benefits. For instance, via the use of cloud computing contractors, organizations can shift portions of their information technology (IT) budgets from capital formats (long term, high dollar investments) to more predictable operational budgeting approaches based on metered usage (Johnson, 2012). This advantage amplifies the advantages of cloud computing's inherent scalability and elasticity (ability to expand/contract services and resources based on dynamically shifting work requirements). Further, the use of third party cloud contractors shifts the burdens of system administration, security regimes, maintenance/upgrade programs, and disaster recovery services to the contractor (Layton, 2007). This simplifies IT management, and helps to decrease in-house IT workloads. As in-house IT workloads decrease, organizations can achieve cost savings via reduced staffing. Moreover, by shifting rote system management activities to third

parties, organizations can focus their staffing resources more directly on operations that are vital to their business models (Laudon & Laudon, 2014)

To leverage the benefits of third party cloud computing such as those discussed above, organizations must engage in procurement – purchasing cloud services/resources from an outside organization via use of legally-enforceable contracts supported by allocated budgets (Fleming, 2003). In this connection, cloud computing purchases implicate the procurement life-cycle. The procurement life-cycle involves planning, solicitation development, solicitation processing/contract award, contract administration, and contract close-out (Project Management Institute, 2013).

In large measure, the very first phase of the life-cycle -- planning, is the lynch pin for successful cloud computing procurements. In cloud computing contexts, planning must focus on a unique blend of considerations that center on the characteristics of cloud platforms and aligned cloud services (Hon, Millard & Walden, 2012). In line with this assertion, this paper covers the core considerations involved in planning for the procurement of cloud computing services and resources. The discussion draws upon information found in professional and academic literature regarding cloud computing engagements. The overall objective of the paper is to set forth a conceptual framework for planning in this area. The framework and its elements provide inputs and guidance for the downstream phases of the procurement life-cycle. Further, the framework is cast in a prescriptive format. This reflects the action-oriented nature of cloud computing procurement planning.

## Understand the Cloud Deployment Models

To begin the planning process, the organization considers which of the four basic cloud deployment models it will adopt – private, public, community, or hybrid (CIO Council, 2012;

Johnson, 2012). As discussed below, each model differs with respect to ownership of the computing and network infrastructures involved, and the location and management of data contained within the infrastructures. These different characteristics shape and guide the organization's efforts to develop scopes of work and terms and conditions for bid documents and contracts. Scopes of work delineate the technical, service and resource requirements for the prospective bid and contract. The terms and conditions are the specific, legally enforceable provisions of a contract such as warranties of service continuity and data security (Fleming, 2003). Accordingly, when considering cloud computing procurements, it is important for organizations to match their needs and constraints with the characteristics of the available deployment models.

**Public Clouds**

Public clouds are owned and hosted on the premises of third parties – for example, contractors like Google, Amazon or Microsoft or academic institutions. These organizations deploy cloud infrastructures and services for use by the general public and commercial sector. This entails multiple, simultaneous users (multitenancy) for the data and software programs that reside in the cloud infrastructure. The customer has little or no control over the location and management of data maintained in public clouds (CIO Council, 2012; Johnson, 2012; Amos et al. 2014).

**Private Clouds**

In contrast to public clouds, private clouds are dedicated to the uses of a single organization, with the infrastructure being owned and hosted by the user organization, third party or a combination of the two (National Institute of Standards and Technology, 2012). It is worth mentioning here that for private clouds that are owned by the user organization, there is no need

for third-party cloud procurement planning. After all, with private ownership, the organization controls the cloud platform directly. On the other hand, to the extent that the privately-owned cloud serves multiple purposes across different functional units, the organization may find it helpful to use some of the planning elements discussed here to develop responsive in-house cloud computing programs.

**Community and Hybrid Clouds**

Community clouds support computing activities exclusively for a specific group or community of user organizations that share a common purpose, concern or collaboration space. Similar to private clouds, community clouds may be owned/hosted by a member or members of the community, a third party, or combinations of members/third parties (National Institute of Standards and Technology, 2012). Finally, hybrid clouds involve the simultaneous use of two or more of the first three models (public, private and/or community) via the application of standardized interfaces that ensure the hybrid components operate together smoothly (Practice Guide, 2014).

**Procurement Implications**

Relative to procurement best practices in choosing deployment models, professionals in the IT field suggest that organizations consider the relative significance of the applications, infrastructures and functions they wish to move to the cloud (National Institute of Standards and Technology, 2012; Practice Guide, 2014). While there are no strict prescriptions here, it seems logical to conclude that non-sensitive data and systems are most suited for public clouds, while highly sensitive, mission-critical data/systems with severe information disclosure restrictions are logical candidates for private clouds. Organizations seeking to implement community or hybrid clouds can blend the characteristics of private and public cloud provisioning based on the

criticality of the data and systems involved (National Institute of Standards and Technology, 2012; Amos et al. 2014; Practice Guide, 2014).

## Choose the Appropriate Cloud Service Delivery Model

Another key planning element centers on choice of a service delivery model. Like the choice of the deployment model, choice of the service delivery model helps to shape the scopes of work and terms and conditions for bid/contract documents. The National Institute of Standards and Technology (2012) identifies three types of cloud service delivery models. Each model entails specific procurement considerations.

### Software as a Service (SaaS)

Under SaaS contracts, the organization pays for access to an application software suite that can be configured (but typically not customized) to support a generalized function. Examples of these functions include: customer relationship management (CRM); enterprise applications like accounts payable/receivable and general ledger; electronic mail/office productivity software; and various management suites including sales, human resources and content/document management (Practice Guide, 2014). Here, the end user interacts with the application via a browser connected to the Internet. The cloud contractor provides for and administers all aspects of the application environment. This encompasses the application software, software stack (database and operating systems), data storage, and underlying hardware. It also includes all of the services required to keep the applications available, secure and up to date with regard to patches and software versions (Amos et al. 2014).

### Platform as a Service (PaaS)

PaaS contracts focus on the provision of application development toolkits via the cloud. In essence, this model revolves around the contractor delivering a development stack –

application development software suite and the underlying data management environment, which the customer organization then uses to design, build, test and deploy application software (National Institute of Standards and Technology, 2012). Under this model, like the SaaS model, the service provider keeps the stack and underlying infrastructure up to date, secure and available. The resources involved include the database/operating system complex, network infrastructure, processing resources, and data management fabrics (National Institute of Standards and Technology, 2012; Amos et al., 2014).

**Infrastructure as a Service (SaaS)**

IaaS engagements address the organization's needs for readily accessible virtual computers, network-resources and data storage (National Institute of Standards and Technology, 2012). In basic terms, under an IaaS contract, the contractor provides the computing environment – for example, operating systems with processing, memory, network, and storage resources. In this context, while the service provider is responsible for provisioning the resources and ensuring they meet the customer's capacity and performance specifications, the organization must administer the resources directly (National Institute of Standards and Technology, 2012; Amos et al., 2014).

## Define General Service Levels

Planning for service levels is a more detailed or granular process. Service levels are the functional and performance outcomes that organizations seek to obtain from a cloud computing contractor. Hence, defining these elements is a central part of a cloud computing procurement initiative. Ultimately, defined service levels are codified in Service Level Agreements (SLAs) (DeveloperWorks, 2010). SLAs are incorporated into scopes of work in bid documents and contracts. They help organizations evaluate contractors – both during the bidding process and in

connection with administration and auditing of actual performance during the contract period. In essence, they are vital measuring sticks by which organizations assess the quality of bids (evaluation of the bidders' plans and capacities in relation to the required SLAs), and to judge the contractor's actual performance. Further, they factor heavily in contract administration, particularly in billing and payment verification processes (Hon, Millard & Walden, 2012).

**Make-up of SLAs and Examples**

SLAs encompass Service Level Objectives (SLOs). SLOs are measureable metrics or stated objectives/specifications that organizations use to assess the amount and/or quality of cloud services/resources provided during a contract period (DeveloperWorks, 2010; Freedman & Gervais, 2011; Practice Guide, 2014). Amos et al. (2014) and the Cloud Standards Customer Service Council (2015) enumerate several common SLAs/SLOs associated with most cloud computing agreements:

- Service availability (up-time) requirements expressed as percentages of time the service is available for use within defined timeframes (for example, 99.99% during peak shift, between 8:30 a.m. and 5 p.m., weekdays);
- Response time to data queries/report requests (measured in fractions of a second) or to requests for resources like virtual servers and disk storage;
- Security controls such as authentication schema, role-based access regimes, and data encryption requirements designed to prevent unauthorized access, use, dissemination or alteration of data;
- Provisions for disaster recovery and continuity of operations to ensure system availability in the event the cloud service contractor's main computing and network facilities are disrupted;

- Data back-up and restore programs for the restoration of corrupted or lost data items, files, objects or databases;
- Restrictions relative to the location of data (for instance, specifying that data must stay within the boundaries of the purchasing organization's country to meet statutory requirements that prohibit off-shoring of sensitive information);
- Data access privileges that spell out the customers' rights to access and retrieve data/content; and
- Data ownership and transfer rights that ensure the customer can move data from one service provider to another, or back to in-house systems, following contract termination.

**Points of Emphasis for Procurement Efforts**

There are different points of emphasis for SLAs/SLOs under the three cloud service delivery models. For IaaS, the emphasis is on provisioning of infrastructure such as central processing units (CPU), memory, flash storage, disk storage, network channels/capacity, and operating system instances. With PaaS, provisioning of servers – for example, web, data base and application servers, and delivery of database, and software development frameworks are critical (Practice Guide 2014). SaaS focuses on application software availability and performance. Here, the key consideration is to match the functional requirements of the application involved – CRM, sales management, accounts receivable, etc., with the contractor's offering. In doing this, it is important for organizations to remember that little or no customization is possible with SaaS offerings. So, the product's functionality must align closely with the organization's needs, or alternately, the organization may contemplate accepting the provider's business model for the application (Freedman & Gervais, 2011; CIO Council, 2012; Amos et al., 2014; Practice Guide, 2104).

Overall, Johnson (2012) argues that when organizations approach the development of SLAs/SLOs, it would be best for them to view prospective cloud contract engagements as utility-centered endeavors and not as information systems development initiatives. This is due to the pre-configured nature of cloud infrastructures (no need for development of the infrastructures) and the pay-for-use model that cloud contracts are built on. In this regard, one could assert that in defining SLAs/SLOs for cloud computing procurements, organizations should seek to ensure these elements are: relevant to desired performance levels and outcomes; sufficient to achieve the performance levels/outcomes; and measureable for purposes of assessment, auditing and contract management (Freedman & Gervais, 2011; CIO Council, 2012; Practice Guide, 2104; Cloud Standards Customer Service Council, 2015).

## Plan for Cloud Pricing Structure

The pricing structure – how the contractor will bill for services and resources, influences the bid evaluation process. More directly, it serves as the cornerstone or the price/economic competition portion of the process. It also determines the financial viability of the prospective cloud computing contract, and serves as the quantifiable basis for contractor charges. Moreover, it constitutes one of the foundational elements for contact administration activities like billing/payment verifications. Thus, the pricing structure is a critical planning consideration (Johnson, 2012).

In line with these thoughts, cloud computing contractors adopt specific pay-for-use pricing models, which organizations need to understand and plan for. Generally, pay-for-use models shift the funding focus of affected IT infrastructures/services from long-term capital investment perspectives (long-term financing) to operational budgeting models based on estimated usage levels (How Cloud Computing is Influencing, n.d.; Johnson, 2012; Laudon &

Laudon, 2014). As a result, organizations need to work with cloud computing contractors to establish methods to monitor and measure service/resource usage in accordance with agreed-upon metrics and reliable sources of usage information.

**SaaS Structure**

In SaaS implementations, contractors typically measure and bill on monthly, quarterly or annual bases using metrics such as the number of users permitted to access the application(s) involved. However, contractors may also charge for the time an application is in use or the number of times an application feature is executed. Further, SaaS agreements may include usage charges for records processed, network resources consumed, and volume of data stored (National Institute of Standards and Technology, 2012; Moyse, 2015). Of all of the cloud pricing models, the SaaS model remains the closest to the more traditional licensing arrangement. The per-user metric has the merit of simplicity, but it is also potentially inefficient if the user base does not access the SaaS application frequently enough for the organization to derive the full benefits of the cloud service (Moyse, 2015).

**PaaS Structure**

For PaaS, contractors typically measure and charge on monthly, quarterly or annual bases for the number and types of people using the development stack. People who might use/access the PaaS stack include developers and administrators. Also, there are likely to be charges for elements such as data storage, computing (processor) usage, network traffic, resource requests fulfilled – for example, provisioning of servers, and time the platform itself is in use (National Institute of Standards and Technology, 2012).

### IaaS Structure

IaaS billing methods are similar to those used in PaaS arrangements. They include charges for processing, memory, storage and network resource usage. IaaS charges may also include charges for specialized services such as event monitoring and automatic scaling of infrastructure resources based on service demand (National Institute of Standards and Technology, 2012; Moyse, 2105).

### General Considerations

In all cases, organizations must plan to work with contractors to set up assessment/tracking systems that provide for transparency in the measurement of billable resource and service usage (Johnson, 2012). In line with this, it would be wise to plan for the implementation of online dash boards and tables that enhance visualization of usage over time. These resources will enable organizations to develop budget estimates based on modelled usage patterns such as peak and slack processing/network access cycles (Practice Guide 2014).

## Specify Security Requirements

Perhaps more than any other consideration, information system and data security needs drive decisions regarding the adoption of cloud services (Practice Guide, 2014; Cloud Standards Customer Service Council 2013; Taylor, 2015). Broadly speaking, security requirements are designed to assure the integrity, authenticity, availability, longevity, and where indicated, confidentiality/privacy of the organization's data resources. While a detailed treatment of information system/data security programs is beyond the scope of this paper, it will prove helpful to highlight the general components that organizations will likely need to specify in their bid documents and contracts. The security components may be included as SLAs/SLOs as discussed previously and/or under general terms and conditions (Hon, Millard & Walden, 2012).

**Identity Management/Access Control and Data Loss Prevention**

Two basic planning considerations for cloud service agreements center on the inclusion of provisions for identity management/access control (IAMC) and data loss prevention (DLP). IMAC encompasses systematic, controlled and documented processes for vetting end user identifies, and setting up/de-activating user accounts. It also involves role-based access privileges (determining which data resources users may read, modify and/or delete) (Shackleford, 2010). DLP centers on automated, software-based rules that prevent end users from accidentally or intentionally disseminating or disclosing data that is classified as sensitive or confidential to unauthorized parties. Private cloud implementations are most amenable to the use of DLP programs (Shackleford, 2010; SANS Institute, 2015).

**Encryption**

Another critical security feature for the organization's data is encryption. Encryption involves the use of software keys and algorithms to scramble data so that it is incomprehensible to parties who are not authorized to read/modify it, and to render encrypted transmissions readable to authorized parties only (Laudon & Laudon, 2014; Comer, 2015). Ideally, organizations will call on their contractors to provide for encryption while their data flows through network channels (data in transit), and as it is stored within the contractor's facilities (data at rest). An example of a strong encryption process for data at rest is the Advanced Encryption Standard (AES) (Layton, 2007; Comer, 2015; SANS Institute, 2015).

**Security Software**

Academicians and professional organizations confirm that the cloud computer contractor's computing and network facilities should adhere to industry best practices for use of security software, and that accordingly, procurement agreements specify such adherence

(Practice Guide, 2014; Comer, 2015; SANS Institute, 2015). Examples of common requirements include the use of firewalls and intrusion detection/prevention software at multiple levels within the contractor's computing/network facilities. These resources help to prevent illicit data transmissions and malware attacks. In the same connection, cloud computer contractors should install and actively use anti-virus/anti-malware software, with constantly updated virus/ malware definitions to detect and safely remove malicious software code.

**Data Management**

Data management practices are also important parts of the cloud security regime. Here, organizations should look to develop contract provisions that help to ensure cloud-based data is properly safeguarded, retained and disposed of. In line with this, baseline data management provisions cover back-up/restore services, disaster recovery/business continuity programs and data retention/disposition regimes (Layton, 2007).

Back-up/recovery involves the scheduled creation of all data and software programs, coupled with the tested capacity to restore data/programs from back-up media on demand following lose or damage of the customer's system resources (Layton, 2007; Elmasri & Navathe, 2011). From the customer's standpoint, disaster recovery/business continuity programs (DR/BCP) address the cloud computing contractor's ability to assure continual availability of its cloud computing/network resources following a disruptive or catastrophic event (Layton, 2007). Organizations may require contractor's to offer DR/BCP capacities like fail-over. Fail-over systems provide for replication of data, programs and network fabrics over multiple, geographically-dispersed facilities, with the ability to switch services automatically to any of these facilities in an emergency (Laudon & Laudon, 2014).

Data retention/disposition provisions revolve around defined time fames in which data must be maintained in accessible form for operational, legal, or research purposes. Further, these provisions include procedures for authorized destruction of data after the expiration of its associated retention time fame (Blatt, 2012). With regard to destruction actions, the organization should ensure the contractor uses secure erasure techniques on all media containing expired data, which assure that the data is rendered unreadable permanently.

**Monitoring, Physical Security and Employee Integrity**

Other security provisions that organizations can build into their procurement agreements center on processes and resources used to monitor the contractor's computers, networks, facilities and employees. The main thrust of these provisions is to require the service provider to maintain a proactive posture relative to assessing and addressing the security and integrity of its resources on an on-going basis. Computing/network incident and event management provisions focus on use of systems that record all cloud system/network events – for example, failed log-in attempts, port scans, abnormal traffic flows, throughput bottlenecks, etc., and present the information for follow up by the contractor's security and administrative team (Layton, 2007; Practice Guide 2014). Organizations should also plan to specify escalation and notification requirements for incidents involving system breaches/data loss as part of the governance process (discussed later in this paper).

Physical security provisions involve requirements for controlling access to the contractor's computing/network resources. These controls may include guard stations, cameras, identification badges, swipe cards and/or biometric elements that restrict access to cloud platform resources to authorized staff only (SANS Institute, 2015). Requirements for employees focus on the integrity of the people who will be handling the organization's data and running its

software programs and networks. In this area, organizations frequently require mandatory criminal background checks for the contractor's employees (SANS Institute, 2015).

### Compliance Credentials

Organizations that operate in highly regulated and governmental settings are often obligated to follow legally-mandated security/compliance regimes, which involve their IT programs and general information management practices. As a consequence, organizations will be compelled to require cloud computing contractors who serve as operational extensions of their IT programs to show proof that they too meet applicable compliance mandates. For instance, Federal agencies may only employ cloud contractors who are certified as being compliant with the Federal Risk and Authorization Management (FedRAMP) program (Taylor, 2015). Behm (2003) outlines other key compliance regimes that may affect cloud procurement initiatives. These include the Federal Information Security Management Act (FISMA), U.S. Privacy Act, the Health Insurance Portability Accountability Act (HIPAA), Sarbanes-OxleyAct, Gramm-Leach-Bliley Act, and the Payment Card Industry Data Security Standard (PCI-DSS) framework.

## Specify Cloud Service Operation Requirements

Service operation requirements are designed to articulate the scope and quality of the contractor's daily management of the cloud computing/service platform, and are therefore key procurement planning considerations. In this area, policies, procedures, communications channels, controls and quality measurements/credentials are of paramount importance. As with security requirements and other elements of the procurement planning process, requirements for service operations can be delineated in SLAs/SLOs or in the terms and conditions of bid documents and contract provisions (Hon, Millard & Walden, 2012; Practice Guide, 2014; Cloud Standards Customer Service Council 2013). The service operation can be a key evaluation factor in the solicitation process (differentiating competitors along quality-of-service lines), and also

facilitate contract administration via the establishment of clear lines of communication and documentation regimes. (Practice Guide, 2014).

**Customer Support**

Customer support revolves around services that the contractor makes available to the customer for routine and non-routine issues, questions and problems, which arise during the course of the contractual engagement. Remote service desks with telephone and online communications channels are most common in cloud service arrangements (Practice Guide, 2014). Examples of typical support problems/matters include requests for application or platform access, feedback relative to outages, complaints about performance bottlenecks, and requests for guidance on software feature usage (Cloud Standards Customer Service Council 2013).

Requirements for customer support emphasize the communications pathways such as telephone numbers, web/chat sites, community knowledge sites/content stores, and electronic mail addresses, along with the specified days/hours of operation (Practice Guide, 2014). Other key performance metrics and features in this area encompass: required problem response/resolution timeframes; percentage targets for successful case resolution; targets for average telephone on-hold time; upper limits for the number of unresolved cases; and escalation schemes (procedures for moving reported problem cases to staff with different levels of expertise) (Open Guide, n.d.). In terms of certifications, the Information Technology Infrastructure Library (ITIL) for individuals and the International Standards Organization (ISO) 20000 framework for organizations are common requirements for IT service operations, including cloud environments (Practice Guide 2014).

### Change/Configuration Management and Integrity/Quality Checks

In general IT contexts, change management involves the roles, responsibilities, procedures, and templates/documents used to implement approved changes in a controlled fashion (Layton, 2007). In line with this, configuration management centers on tracking and deploying versions of a particular set of IT components to ensure smooth system operations (Project Management Institute, 2013). For cloud service engagements, the organization will need to specify its expectations regarding the contractor's responsibilities for keeping software up to date and patched, and to provide ample notice of required service downtime for routine changes/maintenance (Practice Guide, 2014; Cloud Standards Service Council, 2015).

Integrity/quality checks focus on requirements for independent validation of the soundness of the service provider's operations. Generally, organizations address this component of the engagement by requiring the contractor to undergo periodic audits by third party firms that focus on compliance with security best practices. These include requirements set forth under the ISO 27001 security framework, specifications for data center operations listed in the Statement on Standards for Attestation Engagements Number 16 (SSAE 16), and conditions for service quality under ISO 9001 (Layton, 2007).

## Plan for Contract Governance/Administration

Planning for the governance/administration of cloud computing contracts is a key to ensuring successful procurements and effective on-going engagements (Hon, Millard & Walden, 2012; Practice Guide, 2014). Planning for these elements also provides a foundation for effective contract closure processes. Typically, the organization's fiscal or procurement office will handle this aspect of the effort. Activities in this area include general oversight and bill verification/payment.

**General Oversight**

General oversight includes designating staff to monitor the contractor's performance on an on-going basis, and to negotiate changes to the contract if necessary. It also involves delineating notification protocols for outages and unresolved problems, as well as data breach/loss reporting – a very sensitive matter with respect to legal liabilities, financial exposure and brand image (CIO Council, 2012; Practice Guide, 2014). Moreover, the organization will need to determine which of its staff members will be assigned the responsibility for monitoring for compliance with the terms and conditions of the cloud computing contract. The detailed specification and finalization of these terms and conditions occur later in the procurement cycle – during the solicitation development and contract award phases (Fleming, 2003). Suffice it to say here that the terms and conditions include considerations like desired contractual warranties relative to conformance with cloud operations and SLAs/SLOs, and remedies for failure to meet the specified warranties (CIO Council, 2012; Hon, Millard & Walden, 2012; Practice Guide, 2014). The latter may cover excused and unexcused breaches of warranty – specific circumstances that are outside or within the control of the service provider respectively, and the proposed monetary penalties for unexcused breaches.

The organization must also spell out the circumstances that enable it to terminate (close) the contract, and set forth the monetary limitations on contractor reimbursements under a termination scenario (Amos et al., 2014). Further, the termination provisions must allow for a transition period that allows the organization to transfer its data and resources to another service provider, or back to its own IT platform (Hon, Millard & Walden, 2012; Cloud Standards Customer Service Council, 2015). These provisions help the organization ensure the continuity and integrity of its IT systems and data management operations.

### Bill Verification/Payment

In this area, the organization plans to staff a function assigned the responsibility for reviewing billable activity as it occurs, and for verifying bills. Here, the organization plans for using reporting mechanisms to verify that the contractor's billings are accurate. It also plans for allocating staff time to processing payments under the terms of the contract, and storing records pertaining to all verification/payment activity (Practice Guide, 2014; Amos et al., 2014). The key to success in this area is to establish administrative functions that ensure only agreed-upon billing categories are used and that billed items match usage levels. These functions are also designed to take into consideration any contractual penalties that may apply for warranty breaches or defaults (CIO Council, 2012; Johnson, 2012; Practice Guide, 2014).

## Specify Data Management Requirements

This planning element addresses issues such as ownership of cloud-based data and intellectual property, both during and after the termination of the contract. These elements align with security, data location/protection, compliance, and service operation requirements, and are articulated in bid documents and contract terms and conditions. They also connect with and are implemented through the governance/administration structure detailed earlier (Hon, Millard & Walden, 2012; Practice Guide, 2014).

### Data Ownership

Trappler (2012) recommends that organizations plan to include provisions in their service agreements that address different dimensions of ownership. This entails the use of language that reserves all rights, titles and interests to any of the organization's cloud-based data. It may also include rights to the outputs or results of any processing of cloud-based data. Overall, the organization should seek to develop provisions that strictly limit the contractor's data access

rights to actions aimed at meeting contractual duties only (Trappler, 2012; CIO Council, 2012; Johnson, 2012; Practice Guide, 2014).

In the same way, organizations should plan to protect their rights to intellectual property maintained in the cloud. Intellectual property includes content that is copyrighted or protected – for example, software programs, licenses or unique work methods that the organization has or is attempting to patent or protect. Here, the organization plans to build in protections such as provisions that provide for injunctions against unauthorized sale or disclosure of protected data/content, and specifies monetary penalties for violations of the intellectual property terms (Intellectual Property in the Cloud, 2013).

**Discovery**

Discovery processes include the activities required to access, segregate and preserve data for use in audits, investigations and legal proceedings (The Sedona Conference, 2007). This specialized area is a concern for organizations because of the potential for fines and/or adverse rulings and findings associated with non-responsiveness to requests for data under the organization's legal custody. As a consequence, it is important for organizations to plan for the incorporation of discovery provisions into their cloud service contracts. Generally, the requisite provisions require the contractor to be able to respond to litigation hold orders issued by the organization (orders to stay any destruction actions) regarding specific classes and ranges of data pertaining to a particular investigatory or legal matter (The Sedona Conference, 2010). A related consideration is the structuring of provisions that limit, within the bounds of applicable laws, the disclosure of data requested by third parties – persons or organizations outside of the contracting organization (The Sedona Conference 2010).

**Data Migration**

Data migration may involve three flows – data flowing from the organization's internal or in-house platforms to the cloud contractor's facilities, reverse flows from the contractor back to the organization, and flows from one contractor to another (Practice Guide, 2014). The first type of flow occurs when the organization has legacy data that must be housed in the contractor's infrastructure for prospective cloud-based use. In this area, the organization will need to plan for the specification of the migration software, security methods like encryption, and transmission channels that it intends to use to effectuate the migration. Planning for applicable transmission fees and support services may also be required here (Practice Guide, 2014).

The second type of flow, contractor-to-organization, may occur routinely – for example, as part of a redundant data back-up regime, and/or following termination of a service arrangement. The considerations involved for routine reverse flows are largely the same as for organization-to-contractor flows. However, the flows following termination are more involved. In planning for post-contract-termination data migrations, the organization will need to anticipate the invocation of the data ownership/contract termination and transition provisions discussed previously. The organization must also be prepared to structure provisions that ensure the contractor is required to provide all requested data (complete coverage) (Practice Guide, 2014). Trappler (2012) and the Cloud Standards Customer Service Council (2015) note that organizations should specify in advance: when they wish their data to be returned (deadlines); the format the data must be in (compatibility with the organization's infrastructure is of paramount importance); whether and for how long the organization's data will reside on the contractor's infrastructure after termination of the contract; and instructions for securely erasing or obliterating back-up data stored on the contractor's infrastructure. Brandel (2009) and Small

(2012) emphasize that due to compliance, brand image and intellectual property considerations, failure to plan for such post-termination processes can have serious deleterious consequences for organizations, especially in relation to unauthorized disclosure of data following contract termination.

Finally, provider-to-provider data flows may occur when the organization switches from one contractor to another following contract termination, or following the sale of a contractor's operations and/or assets to a different contractor (Cloud Standards Customer Service Council, 2015). In these situations, the organization will need to develop provisions that hold the initial contractor responsible for effectuating the data transfer within clearly delineated timeframes securely, completely, and in the proper format for ingestion into the new contractor's platform. Additionally, similar to termination scenarios, in the event of a sale, the organization should plan to develop provisions that require the contractor to support the organization during a specified transition period (Cloud Standards Customer Service Council, 2015). Here, in addition to helping the organization ensure the continuity and integrity of its IT systems and data management operations, the transition will allow time for the contacting process for the new cloud computing engagement to unfold.

## Conclusion

This paper explored the core considerations associated with the planning process for cloud computing procurements. Drawing upon information presented in professional and academic literature, it surfaced best practices for planning these specialized procurements. The discussion centered on the development of a prescriptive conceptual framework that featured cloud procurement planning elements. The elements included cloud deployment/service models, SLAs/SLOs, pricing, security, service operations, contract governance/management, and data

management. Finally, the paper highlighted how the planning framework serves as the starting point and foundation for the entire cloud computing procurement life-cycle.

## References

Amos, S., Barlow, J., Beam, T., Bertolini, P., Bittner, K., Booth, B., …Melody, R. (2014). *Best practices guide for cloud and as-a-service procurement. Center for Digital Government.* Retrieved from http://cms.erepublic.com/common/resources?product_id=799&appCore=%2Fcommon%2Fforms%2Fajax_form%2F799

Behm, R. L. (2003). The many facets of an information security program. *SANS Institute*. Retrieved from http://www.sans.org/reading-room/whitepapers/awareness/facets-information-security-program-1343

Blatt, R. (2012) *Considerations for content management systems*. Retrieved from http://nagara.org/images/downloads/2012___2013_LG_Records_Management_Bulletins/considerations_for_content_management_systems___edited_20130831.pdf

Brandel, M. (2009). Cloud computing: Don't get caught without an exit strategy. *Computerworld.* Retrieved from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128665&source=NLT_AM

Comer, D.E. (2015). *Computer networks and internets.* (6th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

CIO Council and Chief Acquisition Officers Council. (2012). *Creating effective Cloud computing contracts for the federal government best practices for acquiring IT as a service*. Retrieved from https://cio.gov/wp-content/uploads/downloads/2012/09/cloudbestpractices.pdf

Cloud Standards Customer Service Council. (2013). *Migrating applications to public cloud services: Roadmap for success*. Retrieved from http://www.cloud-council.org/deliverables/CSCC-Migrating-Applications-to-Public-Cloud-Services-Roadmap-for-Success.pdf

Cloud Standards Customer Service Council. (2015). *Practical guide to Cloud service agreements version 2.0.* Retrieved from http://www.cloud-council.org/deliverables/CSCC-Practical-Guide-to-Cloud-Service-Agreements.pdf

DeveloperWorks Cloud Computing Editors IBM. (2010). *Review and summary of cloud service Level Agreements.* Retrieved from http://www.ibm.com/developerworks/cloud/library/cl-rev2sla-pdf.pdf

Elmasri, R. & Navathe, S.B. (2011). *Fundamentals of database systems*. (6th ed.). Upper Saddle River, NJ: Pearson Education, Inc.

Fleming, Q. W. (2003). *Project procurement management, Contracting, subcontracting, teaming.* Tustin, CA: FMC Press.

Hon, W. K, Millard, C. & Walden, I. (2012). Negotiating cloud contracts: Looking at clouds from both sides now. *Stanford Technology Law Review 16*(1), pp. 79-129. Retrieved from https://journals.law.stanford.edu/sites/default/files/stanford-technology-law-review/online/cloudcontracts.pdf

How Cloud computing is influencing procurement. (n.d.). In *Beeline.* Retrieved from https://www.beeline.com/blog/cloud-computing-influences-procurement/

Intellectual property in the cloud. (2013), In *Allen & Overy LLP*. Retrieved from http://www.allenovery.com/SiteCollectionDocuments/Intellectual_property_in_the_cloud_May_2013.PDF

Johnson, J. M. (2012). Procuring the cloud: Shifting to a "utilization" model of IT. *Contract Management, 52, 20-29*. Retrieved from http://search.proquest.com/docview/1722656451?accountid=8289

Layton, T.P. (2007). *Information security: Implementation, measurement and compliance.* (2nd ed.). Boca Raton, FL: Auerbach Publications Taylor& Francis Group.

Laudon, K.C. & Laudon, J.P. (2014). *Management information systems: Managing the digital firm.* (13th ed.). New York, NY: Pearson.

Moyse, I. (2015, April 10). *Cloud billing models in 2015 and beyond.* Retrieved from http://cloud-collaboration.kahootz.com/cloud-billing-models-in-2015-and-beyond

National Institute of Standards and Technology. (2012). *Cloud computing synopsis and recommendations, Special publication 800-146.* Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-146.pdf

Open guide, Service desk. (n.d.). In *ITIL.org*. Retrieved from http://www.itlibrary.org/index.php?page=Service_Desk

Practice guide on procuring cloud services for Hong Kong, Guangdong published. (2014, Dec 5). *Hong Kong Government News.* Retrieved from http://search.proquest.com/docview/1630249070?accountid=8289

Project Management Institute. (2013). *A guide to the project management body of knowledge (PMBOK guide).* (5th ed.). Newton, PA: Author.

Freedman, B. J. & Gervais, B. L. (2011). Procuring cloud computing services in Canada. Retrieved from http://search.proquest.com/docview/897000122?accountid=8289

SANS Institute. (2015). *Critical security controls, Version 5*. Retrieved from https://www.sans.org/critical-security-controls/controls

The Sedona Conference. (2007). (2nd ed.). *The Sedona Principles: Best practices, recommendations & principles for addressing electronic document production.* Sedona, AZ: Author.

The Sedona Conference. (2010). *Commentary on legal holds: The trigger & the process.* Sedona, AZ: Author.

Shackleford, D. (2010). Cloud security and compliance: A primer. *SANS Institute*. Retrieved from https://www.sans.org/reading-room/whitepapers/analyst/cloud-security-compliance-primer-34910

Small, M. (2012). Cloud computing deadly sins. *Database & Network Journal, 42(*5), p26.

Taylor, L. (2015, February 15). FedRAMP: History and future direction. *Cloud Computing, IEEE, 1* (3), pp. 10-14. DOI: 10.1109/MCC.2014.54

Trappler, T. J. (2012, January 17) *When your data's in the cloud, is it still your data?* Retrieved from http://www.computerworld.com/article/2501452/data-center/when-your-data-s-in-the-cloud--is-it-still-your-data-.html