LEGAL NOTICE

© 2014 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.

This “Open Data Center Alliance™ White Paper: Procurement of Cloud Services” document is proprietary to the Open Data Center Alliance (the “Alliance”) and/or its successors and assigns.

NOTICE TO USERS WHO ARE NOT OPEN DATA CENTER ALLIANCE PARTICIPANTS: Non-Alliance Participants are only granted the right to review, and make reference to or cite this document. Any such references or citations to this document must give the Alliance full attribution and must acknowledge the Alliance’s copyright in this document. The proper copyright notice is as follows: “© 2014 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.” Such users are not permitted to revise, alter, modify, make any derivatives of, or otherwise amend this document in any way without the prior express written permission of the Alliance.

NOTICE TO USERS WHO ARE OPEN DATA CENTER ALLIANCE PARTICIPANTS: Use of this document by Alliance Participants is subject to the Alliance’s bylaws and its other policies and procedures.

NOTICE TO USERS GENERALLY: Users of this document should not reference any initial or recommended methodology, metric, requirements, criteria, or other content that may be contained in this document or in any other document distributed by the Alliance (“Initial Models”) in any way that implies the user and/or its products or services are in compliance with, or have undergone any testing or certification to demonstrate compliance with, any of these Initial Models.

The contents of this document are intended for informational purposes only. Any proposals, recommendations or other content contained in this document, including, without limitation, the scope or content of any methodology, metric, requirements, or other criteria disclosed in this document (collectively, “Criteria”), does not constitute an endorsement or recommendation by Alliance of such Criteria and does not mean that the Alliance will in the future develop any certification or compliance or testing programs to verify any future implementation or compliance with any of the Criteria.

LEGAL DISCLAIMER: THIS DOCUMENT AND THE INFORMATION CONTAINED HEREIN IS PROVIDED ON AN “AS IS” BASIS. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE ALLIANCE (ALONG WITH THE CONTRIBUTORS TO THIS DOCUMENT) HEREBY DISCLAIM ALL REPRESENTATIONS, WARRANTIES AND/OR COVENANTS, EITHER EXPRESS OR IMPLIED, STATUTORY OR AT COMMON LAW, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, VALIDITY, AND/OR NONINFRINGEMENT. THE INFORMATION CONTAINED IN THIS DOCUMENT IS FOR INFORMATIONAL PURPOSES ONLY AND THE ALLIANCE MAKES NO REPRESENTATIONS, WARRANTIES AND/OR COVENANTS AS TO THE RESULTS THAT MAY BE OBTAINED FROM THE USE OF, OR RELIANCE ON, ANY INFORMATION SET FORTH IN THIS DOCUMENT, OR AS TO THE ACCURACY OR RELIABILITY OF SUCH INFORMATION. EXCEPT AS OTHERWISE EXPRESSLY SET FORTH HEREIN, NOTHING CONTAINED IN THIS DOCUMENT SHALL BE DEEMED AS GRANTING YOU ANY KIND OF LICENSE IN THE DOCUMENT, OR ANY OF ITS CONTENTS, EITHER EXPRESSLY OR IMPLIEDLY, OR TO ANY INTELLECTUAL PROPERTY OWNED OR CONTROLLED BY THE ALLIANCE, INCLUDING, WITHOUT LIMITATION, ANY TRADEMARKS OF THE ALLIANCE.

TRADEMARKS: OPEN CENTER DATA ALLIANCE™, ODCA™, and the OPEN DATA CENTER ALLIANCE logo® are trade names, trademarks, and/or service marks (collectively “Marks”) owned by Open Data Center Alliance, Inc. and all rights are reserved therein. Unauthorized use is strictly prohibited. This document does not grant any user of this document any rights to use any of the ODCA’s Marks. All other service marks, trademarks and trade names reference herein are those of their respective owners.
OPEN DATA CENTER ALLIANCE™ WHITE PAPER:
PROCUREMENT OF CLOUD SERVICES

EXECUTIVE SUMMARY
Cloud-based services have made the evolution of IT services, and adoption by business consumers and users of these services from various providers, extremely fast and easy. Adopting cloud-based services may provide significant benefits to an organization. For example, these services may enable the organization to rapidly provision its projects and support fast-paced product development and business growth. However, the agility of and easy access to cloud-based services can also introduce challenges for the existing governance structures as they attempt to control and maintain business goal alignment and compliance.

Cloud-based services today are typically designed to be selected, ordered, and committed to by an organization’s business unit or end user, through a cloud service portal. This portal may or may not be within the organization’s authorized service sourcing control. The organization may incur costs and commercial and compliance implications as a result of this commitment. Therefore the organization needs to ensure ongoing commercial and operational compliance and protect its end users, who, in using these channels to adopt cloud services, potentially have unknown capability and power at their disposal.

As a result, it is of interest to the procurement group to actively participate in this service initiation chain and to retain control of it and the associated financial commitments and commercial relationships that may accompany it. In some organizations this function may be distributed and in others centralized, but in all models a formal procurement function that coordinates financial and commercial obligations with external parties is seen as good practice. However, the procurement group may need to review its existing processes to be able to both support cloud service adoption and the associated enablement for the organization and successfully achieve business objectives.

Once the IT and procurement processes have been reviewed (as may be needed) to incorporate the facilitation of cloud-based services, they should be well positioned to enhance and coordinate the effective adoption of cloud-based services for the organization.

This white paper describes how corporate procurement and contracting processes can be updated to better deal with procurement of cloud-based services. These updates are designed to help organizations successfully procure and control cloud-based services in an ongoing, sustainable, efficient, and compliant manner. Following the best practices recommended in this paper may help organizations align risk and reward decisions, enabling them to balance value with control, agility with governance, and freedom with accountability.
Changes to the Traditional Procurement Process

Cloud-based services and their procurement method drive a number of fundamental changes to an organization’s central procurement process. Organizations can handle these changes in a number of ways using various models of federated procurement processing or centralized processing. It is up to each organization to determine the most appropriate process. For illustrative purposes, this white paper focuses on centralizing as much as possible the procurement process for cloud-based services. Each organization should be able to define its own applicable derivatives from this framework.

Traditional Procurement Process

Traditionally, IT procurement has generally been based on the positioning of the IT group as a gatekeeper to all IT-related services. In this role, IT filters, consolidates, and standardizes services, solutions, and investments.

The domain of the IT group typically controls the following areas:

• Technology procured
• Range of services offered to the business units
• Location of services and who provides them
• Renewal of technology elements as required
• Adoption of new technology functions and features

After the IT group approves solution requirements and passes them to the key supporting organizational units—procurement and finance—the following steps are usually taken:

1. Procurement processes any asset or service requirements to be fulfilled externally against the planned IT budget (capital expenditures (CAPEX) and operational expenditures (OPEX)).
2. Procurement writes a request for information and later a request for proposal (with input from IT).
3. Procurement, using a compliant process, selects providers and suppliers.
4. Procurement and finance negotiate contracts with the selected providers and suppliers for the provision of services, for an agreed period, and usually based on defined revenue flows and service scopes.

Once these steps are completed, the service and element delivery is planned (usually against milestones), provision and service integration occurs, and eventually the business user receives the resulting capability or capacity originally requested from IT.

Updated Cloud-Aware Procurement Process

With cloud-based services, the business user can directly contact a cloud service provider portal or interface in real time, select from the services available online, and commit to the terms and conditions of use. The services are then instantiated immediately and are accessible to the business user over a (public) network. IT or procurement may not know about these services until an invoice arrives, or if the invoice is delivered directly to the business user, they may never become aware of the services.

This significant change in the procurement process can potentially lead to value leakage, control breakdown, inconsistent service models, and uncontrolled cloud sprawl (see the Risks Arising from the Non-Cloud-Aware Procurement Process section). However, after leveraging some of the identified updates to the procurement model recommended in this white paper, the organization should be in a better position to efficiently and centrally facilitate the managed procurement of cloud-based services, to better enable successful business objective achievement.
Importance of Finance Group Support

To successfully integrate the procurement process changes suggested in this white paper, it may be necessary to obtain the support of the financial executive of the organization, within whose control the procurement function usually resides. The financial executive should understand the business concepts underpinning cloud-based services and how cloud-based services may affect the financial aspects of the business.

As an example, cloud-based services may be considered an OPEX expense, instead of a traditional CAPEX-oriented IT service expense. Also, the business unit, not the central IT and procurement functions, triggers the financial commitments for cloud-based services. In addition, there may be tax implications against the changing financial model, because some countries allow CAPEX to be depreciated, and under certain circumstances some countries also allow OPEX to be depreciated, such as for intellectual property development projects.

Risks Arising from the Non-Cloud-Aware Procurement Process

As stated earlier, if the non-cloud-aware procurement processes and frameworks are used for procuring cloud-based services, the organization may encounter some of the following risks:

- The IT budget dissolves and is restructured and redistributed among the business units, without optimization and efficiency.
- Corporate data protection may not be applied according to corporate compliance requirements.
- Loss of control of data, process, or service may occur.
- The range of partners to the business and the corporate commitments between them is not controlled or known completely at any point in time.
- Systems and data may end up moving out of legal and geographical control perimeters.
- Shadow IT organizations may evolve, without efficiency and formal frameworks, leading to duplication of effort and business-related decisions being made outside of the formal governance processes of the organization.
- There is no clear view of the business application landscape and portfolio available to support audit, legislative, security, and compliance requirements.
- Compliance requirements for procurement may be distributed and reinterpreted among various user communities.
- Partner selection and business negotiation capacity are distributed, leading to value leakage due to fragmented buying and lack of control over commercial negotiations.

Sometimes larger purchasing departments can be slower to act, although they do so with a background of knowledge of the risks associated with uncontrolled and unmanaged change and the contractual problems associated with business users directly buying services. Business users have a different focus (for example delivering a new manufacturing process) and they very reasonably will not take care of the associated business risks such as disaster recovery, licensing, and service resilience. Instead, they may focus on costs and the delivery of their own goals. This approach can potentially (and has in the past) lead to license sprawl, one service (or server) for each business use, and numerous other problems. Business users typically expect the best, most expensive, fastest, and most up-to-date service available.

Creating a clear procurement framework that also supports the use of cloud-based services, and reviewing procurement processes, tools, and governance to manage these services, may mitigate the above risks in a way that better enables the fast provisioning of services to the business, within a known governance, process, and control framework. This balance of having “just the right” governance is a key enabler for businesses adopting cloud computing at a fast pace. The purchasing department will provide strong supplier negotiation and contract management skills that will protect the enterprise against litigation.

To better enable these central organizational functions to retain control of cloud-based service integration, there are a number of important areas to review and potentially update. The review typically considers what is necessary to achieve the expected business benefits of cloud-based service provisioning and then measures existing business unit components against these requirements.
The desired benefits of cloud-based service provisioning (as per the NIST definition for cloud computing) include the following:

- On-demand self-service
- Measured service (pay per use/demand)
- Rapid elasticity
- Resource pooling (multi-tenancy)
- Broad network access

At a business level, these benefits are usually converted into a number of factors, which are listed across the top of Table 1. The procurement-related elements are listed down the side of the table.

**Table 1. Business-level factors relating to the procurement process.**

<table>
<thead>
<tr>
<th>Procurement Elements</th>
<th>Speed</th>
<th>Agility</th>
<th>Business-Level Factors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Rapid Changes</td>
<td>Capability</td>
</tr>
<tr>
<td>Processes (request, approval, authorization, ordering)</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Governance and Policies</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>People</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Tools and Portals</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Payments</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
<tr>
<td>Contracts</td>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

The organization must measure each of the procurement elements against the business-level factors, setting defined targets for each. For example, if speed means “less than two hours from order to service availability,” the organization must identify what potential changes are necessary to each procurement element to achieve the target. Table 2, on the next page, gives an example.

The remainder of this white paper describes the various aspects that relate to contracting cloud-based services in compliance with organizational policies and standards. It also describes in more detail each of the most important topics that procurement must consider. The objective for these descriptions is to support the update of procurement’s contracting frameworks and processes, in the context of cloud-based services.

Of course, actual system integration changes and process and other updates must always be considered in the context of each specific and individual business or organization, and its appropriate requirements.

Generally a good matrix capability in the context of these topics should also result in a higher cloud maturity model (CMM) achievement for the organization.²

---

¹ See [www.nist.gov/manuscript-publication-search.cfm?pub_id=909505](http://www.nist.gov/manuscript-publication-search.cfm?pub_id=909505)

² See [www.opendatacenteralliance.org/ourwork/usagemodels](http://www.opendatacenteralliance.org/ourwork/usagemodels)
Table 2. Sample matrix for aligning business-level factors with procurement elements.

<table>
<thead>
<tr>
<th>Processes</th>
<th>Agility (Rapid Changes)</th>
<th>Business-Level Factors Capability</th>
<th>Quality</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>Current: 2 weeks&lt;br&gt;Target: 2 hours&lt;br&gt;Change required: Update process and automate it via an online workflow or portal</td>
<td>Change required: Update processes for short-term changes, with shorter processes for existing services</td>
<td>Current: Known products are defined annually and form the framework for procurement&lt;br&gt;Target: New products are introduced constantly&lt;br&gt;Change required: Enable online real-time updating using online systems</td>
<td>Current: Paper based&lt;br&gt;Target: Automated online&lt;br&gt;Change required: Defined process is supported by tooling for authorizations, approvals, and workflow</td>
<td>Current: Manual processes, with paper-based movement&lt;br&gt;Target: Online processing, with automated workflows</td>
</tr>
<tr>
<td>Governance and Policies</td>
<td>Current: Weekly review&lt;br&gt;Target: Real-time review&lt;br&gt;Change required: Automated process above must address the governance structures and route approvals accordingly</td>
<td>Change required: Identify the governance that is absolutely necessary, and link these parties into the automated process. For example, change management and financial approval</td>
<td>Current: Centralized control&lt;br&gt;Target: Enriched staff understanding and awareness of governance and control requirements across the organization, to embed greater accountability across the layers</td>
<td>—</td>
</tr>
<tr>
<td>People</td>
<td>Current: Manual processing of paper quotes and requests&lt;br&gt;Target: Automated online approvals&lt;br&gt;Change required: Training and RACI updates</td>
<td>Change required: Training and RACI updates, using automated online workflows</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>Tools and Portals</td>
<td>Current: Internal order portal for standard office items&lt;br&gt;Target: Cloud service ordering integrated&lt;br&gt;Change required: Align with IT and providers, and create an integrated procurement portal and workflow, right through to the cloud providers</td>
<td>Change required: Update portals to allow authorized changes to running services online, supported by online governance</td>
<td>Current: Fixed products are annually defined in a catalog&lt;br&gt;Target: Catalog can be updated online in real-time&lt;br&gt;Change required: Bring catalog and update process online, and automate updates</td>
<td>—</td>
</tr>
<tr>
<td>Payments and Finance</td>
<td>Current: CAPEX management&lt;br&gt;Target: Majority OPEX&lt;br&gt;Change required: Update approval and budget frameworks, and move from fixed to variable costing</td>
<td>Change required: Update payment models to convert from monthly numbers to actual hourly-based service element consumption, with beneficial rates applicable under certain conditions</td>
<td>—</td>
<td>Current: Payment per solution&lt;br&gt;Target: Cost per standard element; define standard element and costs in a catalog to enable accurate benchmarking</td>
</tr>
<tr>
<td>Contracts</td>
<td>Current: Organizational-defined templates; paper-based with committed revenue and services&lt;br&gt;Target: Framework contracts with open service scopes and no revenue commitments; accepted online&lt;br&gt;Change required: Update contract frameworks and bring the relevant parts online including cloud brokerage and cloud exchange support</td>
<td>Change required: Enable fast changes to services, contractually, including new service element additions, and scaling back as well</td>
<td>Current: Contracts define specific products and services&lt;br&gt;Target: Contracts specify frameworks into which new products and services move or are removed dynamically&lt;br&gt;Change required: Update contract frameworks</td>
<td>Current: Solutions defined per demand&lt;br&gt;Target: Standardized&lt;br&gt;Change required: Create a standard service catalog, which can accommodate new and retiring products and capabilities dynamically, filled by service providers and remaining IT services</td>
</tr>
</tbody>
</table>

CAPEX — capital expenditures; OPEX — operational expenditures; RACI — responsible, accountable, contributing, informed

*NOTE: There are several factors that need to be considered to determine whether or not an online contract that’s accepted or approved online by a party will be enforceable under applicable law. Thus, you should seek the guidance of your company’s counsel about steps you may want to take to maximize the enforceability of any online contracts that are accepted or approved online.*
**PROCUREMENT IN A CLOUD-BASED SERVICE LANDSCAPE**

This section discusses in detail each of the topics identified previously. Table 3 provides an overview of the potential differences between traditional corporate service management and cloud-based service use.

Table 3. Potential differences between traditional corporate service management and cloud-based service use.

<table>
<thead>
<tr>
<th>Key Area</th>
<th>Non-Cloud-Aware Procurement</th>
<th>Cloud-Aware Procurement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Processes</strong></td>
<td>IT</td>
<td>Business</td>
</tr>
<tr>
<td></td>
<td>• Collect the requests.</td>
<td>• Find supplier from an Internet or other search.</td>
</tr>
<tr>
<td></td>
<td>• Consolidate and filter requirements.</td>
<td>• Select and configure services, accept terms and conditions, and order services.</td>
</tr>
<tr>
<td></td>
<td>• Write a budget (CAPEX and OPEX).</td>
<td>• Use the services.</td>
</tr>
<tr>
<td></td>
<td>• Pass requests to procurement.</td>
<td>Supplier</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>• Instantiate services that business user configures.</td>
</tr>
<tr>
<td></td>
<td>• Write an RFI and RFP.</td>
<td>• Collect usage data and invoices business user accordingly.</td>
</tr>
<tr>
<td></td>
<td>• Select the supplier.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Develop contract based on standard framework.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Place order for system/services.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pay for services according to milestones.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Pay for maintenance annually.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Supplier</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Deliver services.</td>
<td></td>
</tr>
<tr>
<td><strong>Governance</strong></td>
<td>IT</td>
<td>Business</td>
</tr>
<tr>
<td></td>
<td>• Consolidate all requests.</td>
<td>• Define service requirements and configurations.</td>
</tr>
<tr>
<td></td>
<td>• Align all requests to policies, standards, and budgets.</td>
<td>• Define the service landscapes.</td>
</tr>
<tr>
<td></td>
<td>• Define procurement requirements.</td>
<td>• Report against risk and compliance framework.</td>
</tr>
<tr>
<td></td>
<td>Financial</td>
<td>• Control costs (through demand management).</td>
</tr>
<tr>
<td></td>
<td>• Review investment plan.</td>
<td>• Select cloud service suppliers.</td>
</tr>
<tr>
<td></td>
<td>• Control CAPEX and OPEX.</td>
<td>Supplier</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>• Define service catalog.</td>
</tr>
<tr>
<td></td>
<td>• Define the supplier list.</td>
<td>• Define service terms and conditions.</td>
</tr>
<tr>
<td></td>
<td>• Create defined contract frameworks.</td>
<td>• Deliver services from their infrastructure.</td>
</tr>
<tr>
<td></td>
<td>• Align to corporate budget.</td>
<td>• Report based on predefined elements.</td>
</tr>
<tr>
<td></td>
<td>Risk and Compliance Management</td>
<td>• Calculate costs and invoice user.</td>
</tr>
<tr>
<td></td>
<td>• Define risk frameworks and mitigations.</td>
<td>IT</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define network connectivity.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Classify business applications.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• Define risk management framework and guidelines.</td>
</tr>
<tr>
<td><strong>People</strong></td>
<td>IT Team</td>
<td>Business Users</td>
</tr>
<tr>
<td></td>
<td>• Define corporate services and systems.</td>
<td>• Select services from the suppliers’ portal-based catalog.</td>
</tr>
<tr>
<td></td>
<td>• Restrict business users from straying beyond their defined services.</td>
<td>• Configure services according to their needs</td>
</tr>
<tr>
<td></td>
<td>Business Users</td>
<td>• Order/request service deployment.</td>
</tr>
<tr>
<td></td>
<td>• Request service capabilities and capacity.</td>
<td>• Use the services.</td>
</tr>
<tr>
<td></td>
<td>Risk Management</td>
<td>• Manage services including risk, security, and compliance.</td>
</tr>
<tr>
<td></td>
<td>• Define system security and data protection requirements.</td>
<td>Suppliers</td>
</tr>
<tr>
<td></td>
<td>Procurement</td>
<td>• Define standard services and capabilities.</td>
</tr>
<tr>
<td></td>
<td>• Select suppliers.</td>
<td>• Operate standard services according to defined service parameters.</td>
</tr>
<tr>
<td></td>
<td>• Manage supplier relationships.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Manage contracts and remediation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Select services based on costs.</td>
<td></td>
</tr>
</tbody>
</table>
## Key Area

<table>
<thead>
<tr>
<th>Ports</th>
<th>Non-Cloud-Aware Procurement</th>
<th>Cloud-Aware Procurement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Procurement order portal</td>
<td>• The supplier portal is online (potentially on the Internet) and offers business users a catalog of services that they can select, configure, order, deploy, operate, and change directly.</td>
</tr>
<tr>
<td></td>
<td>• Offer a catalog of available standardized technology elements.</td>
<td>• The portal also contains the terms and conditions for the services, where acceptance (signing) is performed directly, and order numbers/cost centers/credit card details are exchanged in real time.</td>
</tr>
<tr>
<td></td>
<td>• Offer a facility to request non-standard systems.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Provide a workflow facility for request approval.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Integrate into the company intranet.</td>
<td></td>
</tr>
</tbody>
</table>

## Payments

|       | Based on each contract, an order is created and a purchase order issued, against which payments occur. | Based on the actual consumed services, the supplier either debits the credit card of the business user or invoices them against their cost center, on a pay-per-use basis, typically monthly. |
|       | • Maintenance for certain services may be paid additionally on either a monthly or annual basis, against a purchase order number. | • The business user may select “spot pricing” to use against services at different points in time. |
|       | • Monthly payments are predetermined and fixed, often the annual number divided by 12. | • Expenditures move from a CAPEX to an OPEX-based model. Prices are per unit, usually per hour for resources, with “spot pricing” unit opportunities. |
|       | • Unit costs are specific: CAPEX for assets, OPEX for other elements, with clear tax impacts. | • Monthly costs are optimized, but variable, and consist of capital and other cost elements combined, inside of unit charges, which have different tax impacts. |

## Contracting

|       | Procurement defines standard contracts together with the legal department, and these define all of the terms and conditions for service and solutions the suppliers provide. | Terms and conditions for acceptance of standardized services are provided through the cloud portal, by the supplier, and accepted online by the business user. |
|       | • The contracts also define service locations, compliance and legal requirements, payments, service levels, and service remediation regimes. | • Any service remediation is addressed directly between the business user and the supplier, based on the incidents affecting them. |
|       | • Each contract is negotiated and signed separately. | • Contracts are framework-based, with no revenue commitment, and allow for dynamically changing services and rates. The role of cloud brokers is added to contracts, and the use of cloud exchange and cloud trading is enabled. |

CAPEX – capital expenditures; OPEX – operational expenditures; RFI – request for information; RFP – request for proposal

NOTE: There are several factors that need to be considered to determine whether or not an online contract that’s accepted or approved online by a party will be enforceable under applicable law. Thus, you should seek the guidance of your company’s counsel about steps you may want to take to maximize the enforceability of any online contracts that are accepted or approved online.
The comparisons listed in Table 3 indicate that procurement must act as a vital point of consolidation to retain control of supplier spread, manage commercial relationships, and optimize organizational spending and financial commitments.

Typically this means that procurement needs to begin with a survey of the current organization to determine which potential cloud service providers already are providing services, map (together with IT and risk management) potential additional cloud service providers, and then begin to bring these into a structured real-time procurement framework.

The Open Data Center Alliance (ODCA) has created high-level, appropriate questions for requests for proposals (RFPs) against each usage model, which can assist organizations in selecting cloud service providers. These RFP questions are collected in ODCA’s online Proposal Engine Assistant Tool (PEAT).³

The ODCA has also developed a master usage model (ODCA Master Usage Model: Commercial Framework⁴) to guide and optimize the creation of contracts between cloud subscribers and cloud providers. Procurement could consider approaching cloud providers to establish a formal contractual relationship called a master services agreement (MSA), which identifies all cloud service suppliers, formalizes interactions, and establishes governance, process, fulfillment management, and tracking.

The MSA may help to leverage both the organization’s standard terms and conditions, and any specific terms and conditions per service type, governing law, location restrictions, and so on. Some of these aspects or drivers, as per the ODCA Commercial Framework (where much more detail may be found), include those shown in Figure 1. Appendix A – Master Services Agreement provides more detail about the contents of the MSA.

---

Master Service Agreement Components

<table>
<thead>
<tr>
<th>Cost and Service</th>
<th>Trust and Sustainability</th>
<th>Data</th>
<th>Dealing with Issues</th>
<th>Baseline Details within a Contract</th>
</tr>
</thead>
<tbody>
<tr>
<td>- Cost Management</td>
<td>- Privacy</td>
<td>- Ownership</td>
<td>- Incident Management</td>
<td>- Governing Law</td>
</tr>
<tr>
<td>- Service Levels</td>
<td>- Intellectual Property</td>
<td>- Trans-border Flow</td>
<td>- Breach Management</td>
<td>- Subcontracting</td>
</tr>
<tr>
<td>- Availability</td>
<td>- Information Security</td>
<td>- Sanitization</td>
<td>- Electronic Delivery</td>
<td>- Variations to Terms</td>
</tr>
<tr>
<td>- Multi-tenancy</td>
<td>- Portability</td>
<td>- Liability</td>
<td>- Electronic Delivery</td>
<td>- Priority of Documents</td>
</tr>
</tbody>
</table>

Figure 1. Components of a master services agreement.

---

³ www.opendatacenteralliance.org/ourwork/proposalengineassistant
⁴ www.opendatacenteralliance.org/library
Procurement should also consider the following activities:

- Establish an online order workflow and request approval process, operating in real time or as per business requirements
- Establish a financial control and payment framework that aligns to organizational cost centers, budgets, and commercial requirements
- Update the existing corporate order portal with either the various cloud suppliers’ service catalogs or by adding links to the suppliers cloud service portals from the official organizational order portal (to enable service configurations), with pre-selected services and configurations defined (to meet risk and compliance requirements)
- Communicate the availability of these options, with IT, to the business
- Manage the financial flows of invoices and payments
- Establish supplier management forums, with IT and the business
- Collect reporting for financial and budget planning

As stated in the ODCA Master Usage Model: Commercial Framework:

“Cloud services are designed to fulfill a need for flexible use so that a user-company can cope with unplanned requirements in either facilities or volumes. For example, after installing a new system a few months may pass before the customer realizes the cloud can and should be interconnected to another system. For this reason, ODCA suggests all components of an MSA should be discussed and agreed upon, even if some are not in the initial scope. These components can be invoked at a later date, when they are needed.”

It is also important to consider that with cloud-based services, no procurement activity is a single-time event. All of the aspects described above are in the context of an ongoing cloud-service lifecycle, as shown in Figure 2, potentially reinvoking a procurement activity.

**CONCLUSION**

Based on the contents described in this white paper, it is expected that a procurement group should be in a position to analyze its current status, then identify any possible gaps between that and the future state required to enable cloud service procurement and change management in real-time.

Different models exist relating to distributed and centralized procurement functions and how they are currently deployed. Each organization has to select an appropriate model for itself, leveraging and potentially enhancing its current functions, for example, possibly distributing agents to various organizational areas, among other approaches.

The capability for enabling procurement and the central organizations to stay in control of cloud-based services can be achieved relatively quickly, once a review and analysis of the existing procurement processes and frameworks are performed, potential priority development areas identified, and a formal change initiated.

From the recommended gap analysis step, any cultural, paradigm, process, and system change needs may be identified, along with any necessary contract framework updates.

Typically, a formal project should guide the process of addressing these potential changes, as part of the overall cloud-based service integration strategy implementation across the business. This project should be led by a strategy document for adoption of cloud-based services to enable business transformation (See the ODCA Usage Model: Business Strategy Enabling Business Transformation).

Addressing these prerequisites should effectively position procurement to proactively facilitate and enable the business for cloud-based service adoption.

---

5 See [www.opendatacenteralliance.org/library](http://www.opendatacenteralliance.org/library)
6 See [www.opendatacenteralliance.org/library](http://www.opendatacenteralliance.org/library)
APPENDIX A – MASTER SERVICES AGREEMENT

LEGAL DISCLAIMER
Open Data Center Alliance, Inc. is NOT a law firm.

The terms and conditions set forth in this “Procurement of Cloud Services” document are intended to be used as templates only and are not intended as legal advice. Our publishing of this document and your use hereof is NOT intended to create nor does it create an attorney client relationship between Open Data Center Alliance, Inc. and you. We encourage you to seek proper, independent legal advice from an appropriate advisor before making use of any terms, conditions or other materials found herein.

No template can possibly contemplate every contingency, and the particular facts and circumstances of your situation may make an otherwise relevant document undesirable or incomplete. Further, laws and the application of laws by courts and government agencies change frequently. If you use a document, you do so at your own risk and you are totally and solely responsible for the consequences of your actions.

The terms, conditions and other materials set forth in this document are provided to you on an “as is” and “as available” basis. We expressly disclaim all warranties with respect to the content hereof, express and implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. We expressly disclaim any warranty that any terms, conditions or other materials contained herein are legally enforceable. Finally, we reserve the right to change this document at any time in our sole discretion.

The following sections describe the prospective sections of a master services agreement (MSA):

Governing law
This section describes the considerations associated with which law governs the execution, implementation, and fulfilment of the contract. This section also provides information on which laws may be relevant in court cases.

Choices of law and jurisdiction clauses are frequently included in contractual agreements. It is likely that more than one legal jurisdiction will apply to a cloud-based service. The choice of law and jurisdiction will determine which country’s law applies to compliance obligations, dispute resolution, arbitration, etc.

Cloud subscribers usually avoid enforcing contractual terms in overseas jurisdictions under foreign law. Similarly, subscribers avoid defending an action in an overseas jurisdiction under foreign law.

The cost of legal considerations should be assessed and compared with the benefits of the particular cloud-based service in a foreign jurisdiction.

Variations to terms of service
This section provides the considerations to guide how terms and conditions within a contract can be changed, who can make changes, and when the changes can be made.

Multiple parties and subcontracting
This section describes the considerations associated with managing the contracting of services with multiple parties, and subcontracting issues.

Assignment and divestiture
This section describes the considerations for managing the continuity (or otherwise) of a commercial contract when one or more parties to the contract change their business model or organizational structure due to mergers, acquisitions, and divestiture of business interests.
Priority of documents
This section governs which parts of the agreement override other parts of the agreement if there is a conflict between the constituent parts. Such conflicts could occur within a contract or MSA when it has been drafted by multiple stakeholders, when there are many schedules or agreements (master agreement, local agreement, project agreement, schedules, and appendices), or when certain terms and conditions contradict each other.

Intellectual property
This section describes the considerations associated with managing intellectual property (IP) within cloud arrangements. IP protection is applicable for both the cloud subscriber and the cloud service provider. Certain IP rights belong to the cloud subscriber, usually based on the data owned by them. Certain IP rights belong to the cloud service provider, such as algorithms, patents, and design.

Liability
This section describes the considerations associated with managing cloud service provider and cloud subscriber liability.

Indemnification
This section describes the considerations associated with managing the contract’s indemnity clauses. An indemnity commits that one party undertakes to accept the risk of loss or damage the other party may suffer as a result of events, behavior, incidents, or security breaches. The indemnity is a legally binding commitment.

Auditability
This section describes how right of audit and certifications of the cloud service provider should be handled.

Description of services and service-level agreements
This section specifies the principles and requirements to define quality service descriptions and service-level agreements (SLAs).

The commercial framework and contract for a cloud arrangement should clearly define how the services in scope will be provided. The framework should also define how the SLA should be written to augment effective and efficient provision of the services. The SLA section within a contract forms the fundamental basis for:

• Service definition
• Pricing
• Delivery
• Monitoring
• Billing
• Governance
• Remediation and rectification upon non-delivery of agreed-upon services or service qualities

A service-offering item is a product or service that can be ordered from and delivered by the cloud service provider.

An SLA defines the interaction between a cloud service provider and a cloud service subscriber, and should be formalized within the master service agreement or a contract.

Further information on defining and monitoring the security service levels in a cloud contract can be sourced from “Procure Secure: A guide to monitoring of security service levels in cloud contracts,” developed by the European Network and Information Security Agency (ENISA).

Availability
• Availability is defined as the percent of time a system is up and performing at an acceptable level.
• Availability is defined for the whole service.

Cost management
Cost management describes the commercial terms and conditions influencing the management of the cost of services within a cloud arrangement.

Multi-tenancy
Multi-tenancy is the property of multiple systems, applications, or data from different organizations hosted on the same physical hardware. A tenant can be any company or department within a company or application, either inside or outside a single enterprise that needs its own secure and exclusive virtual computing environment.

Privacy
Information privacy is promoted throughout the cloud lifecycle through proper and consistent data classification and collection, proper data processing, communication of private information appropriately, and proper use, storage, and disposal of personal or personally identifiable information.

Information security
Information security’s goal is to ensure that only authorized parties have access to specified information services. Typically controls over information and information systems are in place to ensure:

- Only authorized access and use
- No disclosure
- No disruption
- Only authorized modification and data
- Destruction

Information and services in a cloud must be protected to provide confidentiality, integrity, availability, and non-repudiation, among other qualities.

Data ownership
This section defines ownership rights to data and clear requirements to be specified in a commercial contract.

Data location and cross-border flow
This section describes the implications of choosing a data storage location and moving data from one jurisdictional environment to another, across states, or national borders. Data in the cloud can potentially be anywhere in the world. Data may be stored in multiple data centers. There may also be multiple copies of the data. Sending and processing data around the globe requires compliance with data protection and privacy laws in all of the countries involved. The legal term for this is “trans-border data flow.”

Monitoring by cloud provider/supplier
The cloud service provider may monitor the use of cloud-based services for different purposes. This section specifies the level of monitoring appropriate for a specific usage scenario or context.

Incident management
Incident management and response involves an organized method for dealing with production incidents impacting service levels or the consequences of an attack against the security of a computer system. Incident response refers to activities addressing breaches of systems, leaks/spillage of data, and unauthorized access to data.

Security breach management
The term “breach” covers data that is stolen, infringed upon, disclosed, or altered.
Electronic discovery

Electronic discovery involves the identification, collection, processing, analysis, and production of electronically stored information (ESI) in the discovery phase of litigation. The request for information to support electronic discovery can take the form of subpoenas, search warrants, court orders, public records requests, or request for voluntary disclosure of information.

This section provides guidance to support the handling of Electronic Discovery within Cloud contracts. Further information and related reading on Electronic Discovery and Security can be referenced from “Guidelines on Security and Privacy in Public Cloud Computing, NIST Special Publication 800-144.”

Data sanitization

Data sanitization is the process by which data is irreversibility deleted or removed from media, or the storage is suitably destroyed. Sanitization is undertaken to prevent unauthorized disclosure of information. It is generally applicable when storage is removed from service or moved to another storage location.

This section describes the need to comply with data sanitization and destruction requirements. These requirements are defined by regulatory mandates and the business needs of organizations.

Record retention

This section describes the process to manage record retention requirements, in response to business and regulatory drivers and obligations.

Portability and termination

This section describes the process to manage portability and dealing with cloud termination, in response to business and regulatory drivers.

Software entitlement management

Software entitlement management is the process of managing the pool of software licenses held by an organization [licensee] to ensure that the licensee is not in breach of its entitlement.

---