OPEN DATA CENTER ALLIANCE℠:
SOFTWARE ENTITLEMENT MANAGEMENT FRAMEWORK REV 1.0

TABLE OF CONTENTS

CONTRIBUTORS

The following individuals from the ODCA Regulation, Infrastructure, and Management Work Groups contributed to the contents of this document:

Mick Symonds, Atos

Peter Pruijssers, Atos

Axel-Knut Bethkenhagen, BMW

Nico Steenkamp, Capgemini

Erick Wipprecht, Disney Technology Solutions and Services

Jerzy Rub, Intel

Mrigank Shekhar, Intel

Pankaj Fichadia, National Australia Bank

Tim Palmer, National Australia Bank

Bryon Baker, National Australia Bank

Elisa Li-causi, National Australia Bank

John Llewellyn, National Australia Bank

José González, Trapezoid

Ryan Skipp, T-Systems International GMBH

LEGAL NOTICE

© 2013 Open Data Center Alliance, Inc. ALL RIGHTS RESERVED.

This "**Software Entitlement Management Framework Rev 1.0**" 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: **"© 2013 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.

THE CONTENTS OF THIS DOCUMENT ARE IN NO WAY INTENDED TO CONSTITUTE LEGAL ADVICE AND DO NOT CONSTITUTE THE OFFERING OF, OR PROVIDING OF, ANY LEGAL COUNSELING OR ANY LEGAL OPINIONS. THUS, YOU SHOULD NOT LEGALLY RELY UPON, OR OTHERWISE LEGALLY ACT UPON, ANY OF THE INFORMATION OR CONTENTS OF THIS DOCUMENT WITHOUT FIRST OBTAINING THE LEGAL ADVICE OF YOUR OWN LEGAL COUNSEL.

TRADEMARKS: OPEN CENTER DATA ALLIANCE[SM], ODCA[SM], 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℠: SOFTWARE ENTITLEMENT MANAGEMENT FRAMEWORK REV 1.0

EXECUTIVE SUMMARY

The cloud complicates the effective management of software entitlement, creating investment, usage, monitoring, and optimization issues, as well as introducing risks.[1] These complexities affect cloud subscribers, cloud providers, solution providers, and software vendors and require solutions that are unique to cloud deployments.

To operate in this environment, software users including cloud providers and cloud subscribers must manage their software entitlements while balancing the usage, price, and performance characteristics of software entitlements with the software licensors. The main challenges and complexities include the following:

- Traditional software entitlement management schemes lack mechanisms to accommodate cloud deployments.
- Hybrid and complex approaches to the management of software entitlements create additional challenges that must be overcome.
- Software vendors often prefer maintaining direct relationships with customers and enterprises.
- Large numbers of independent software vendors (ISVs) applying diverse licensing schemes increase the transactional overheads, costs, and complexity of managing software entitlements.
- Predicting the licensing costs and managing compliance present ongoing difficulties.
- Within a single platform-as-a-service (PaaS) or software-as-a-service (SaaS) environment, multiple entitlement models and metrics exist for the different constituents. These have to be synchronized and reported, especially since ISV and other support for the different elements may link or associate with them in real time.

The objectives of the ODCA Software Entitlement Management Framework include the following:

- **Optimize efficiency.** Maximize the value gained from software entitlement investment and provide a basis for cost control through commercial dynamics and dialogue, at an affordable price. Standardize the commercial dynamics to shorten the time taken to negotiate compliant and effective contracts.
- **Reduce risk.** Manage and minimize the risks of noncompliance with software entitlement requisites and licensing agreements resulting in compliance and safety. This approach includes specifying the requirements for monitoring compliance, as well as enabling ISV support and maintenance of the software elements.
- **Simplify use.** Simplify the cloud subscriber's transition into and ongoing use of cloud services and improve the flexibility of software utilization to increase business benefits. This approach involves removing the barriers posed by software licensing schemes across in-house and cloud deployments, minimizing administrative overhead associated with entitlement management processes, and recommending software entitlement models designed for scalable and dynamic cloud deployments. Additionally, alignment of the ISVs to a cohesive model to support management and simultaneous reporting of multiple software products (within a single system) driven by different entitlement criteria also aids simplification.

The Open Data Center Alliance (ODCA) Software Entitlement Management Framework recommends requirements, processes, and practices for effective management of software entitlements in enterprise-grade cloud deployments and is targeted to serve the needs of software consumers and software providers.

---

[1]   Refer to the "Framing the Problem" section within this document.

FRAMING THE PROBLEM

Legacy software entitlement arrangements focus on precise use of licenses, typically tied to specific computers, CPUs, users, and so on. This precision does not adapt well to cloud use scenarios in which the cloud subscriber needs both efficient resource use and the capability to increase or decrease software use dynamically, as needed, without verifying the number of licenses at every instance.

The cloud introduces significant complexities in the effective management and optimization of software entitlements for cloud subscribers, cloud providers, solution providers, and software vendors. Table 1 lists some of these areas of complexity.

Table 1. Key areas of concern introduced by the cloud.

Area	Key Concerns
Workload Migration	Application and infrastructure migrations across enterprise data centers and cloud deployments (public, private, community, and hybrid) that occur frequently or in large volumes make it difficult to obtain an accurate inventory of software entitlements and ensure licensing compliance. To be effective, the compute platform must conform to the way the entitlement is measured.
Workload Mobility	Identifying and tracking "compliant" consumption for licensed software products can be difficult given the increased mobility of workloads and the ability to clone virtualized systems. Tracking must encompass multiple instances through the usage lifecycle across enterprise data centers, internal and external private clouds, public clouds, community clouds, and hybrid clouds. Dynamic provisioning of service instances can potentially lead to unintended consequences for software license consumption, cost management (underutilization or overutilization of software assets) and compliance.
Licensing Models	Traditional software entitlement management schemes typically do not correspond well with essential cloud features, such as virtualized infrastructure, elasticity, self service and on-demand consumption. Virtualization creates technical challenges for mapping physical license models to a virtual environment, including the costing models and support methodology proposed by software vendors. It may be difficult or impossible to make full use of a particular software solution cost effectively within a cloud environment. Many "traditional" software entitlement arrangements tie the deployment of the software to physical infrastructure and hardware traits (such as the number of CPUs, cores, geographical limitations, ownership characteristics, and installation instances). This binds the software licenses to the IT environment in which they are used and to a limited capacity. Traditional software entitlement management arrangements often create issues when migrating from in-house (non-cloud) computing models to the flexible infrastructure of cloud environments. Perpetual licenses could have a practical limited lifecycle, because of technical obsolescence in a virtualization, cloud, or grid environment. Mobility between corporate and multi-tenant cloud scenarios also drives changes to license models (for example, from ELA to SPLA) under the laws associated with certain products. The translation of those changes can be very complex and cause far-reaching impacts. Failure of software vendors to address license issues will continue to drive users to solutions with straightforward licenses, including open-source software. Resolving these types of licensing issues is in the vendors' best interests.
Differing Approaches	Favoring simplicity in licensing models, negotiation, contractual terms, provisioning, billing, and recovery of licenses makes it easier to obtain genuine business value from technology investment. It also helps streamline compliance management. Contractual terms and conditions enacted during negotiation can increase complexity during implementation and post-implementation if not considered carefully—both from a technology and business perspective. Extending the service provision across the cloud adds to this existing issue. It can also increase the volume of transactional overhead, increase costs, and complicate processes for the cloud subscriber, cloud provider, and software vendor.
Predictability of Licensing "Costs" and "Revenue"	The ease with which resources can be allocated and dynamically consumed (scaled up or down) in the cloud creates challenges when predicting the initial and ongoing cost of software licensing. Hybrid license models that encompass usage and device-based licensing models can cause a cloud subscriber to burst limits and breach entitlement agreements, if these models are not managed carefully. Bursting into shared public or service provider-based capacity, from private corporate environments, raises questions of responsibilities and applicable license models. For independent software vendors (ISVs), cloud deployments also make it harder to predict future revenue streams.
Business Relationship	Some ISVs prefer to maintain a direct relationship with whoever is using their software. Others make arrangements so that cloud service providers can "sell-on" the software as part of a service. These ISVs but can still remain directly involved in a defined layer of the back-end support, if they know the identity of the software consumer. Changes to the "use/user" of software often have commercial, relationship, and cost implications.

These complexities influence how cloud subscribers select, adopt, and subsequently manage the cloud environment. Without correctly managed software entitlements, the cloud subscriber or software user could be noncompliant with licensing agreements or contracts and may be open to legal, commercial, or regulatory action with financial and reputational repercussions.

Ineffective management of software entitlements can result in:

- **Financial and commercial risks**, arising from inappropriate use and management of software licenses (under use or overuse of software assets)
- **Regulatory action from government**, causing damage to reputation or resulting in financial penalties (if in breach of export controls)
- **Penalties or legal action by the licensor**, if noncompliance with licensing terms and conditions is demonstrated. Compliance breaches or breach of commercial agreement could, among other consequences, result in suspension of services to the consumer, interrupting business operations and causing subsequent revenue impact.

In the context of this problem statement, the ODCA Software Entitlement Management Framework addresses key issues in unlocking the value of software investment from the perspectives of a software licensor, software licensee, and software user.

TAXONOMY

Table 2 lists the standard terms and definitions used in this document.

Table 2. Terms and definitions.

Term	Description
Cloud Provider	An organization providing cloud services and charging cloud subscribers. A cloud provider provides services over the Internet. A cloud subscriber could be its own cloud provider, such as for private clouds.
Standards Bodies	An entity responsible for setting and maintaining the standards contemplated in this usage model relevant in the context of cloud computing.
Cloud Subscriber	A person or organization that has been authenticated to a cloud and maintains a business relationship with a cloud.
Software Entitlement	This is defined as the software license use rights as defined through agreements between a software licensor and software licensee.
Software License	Legal rights to use software in accordance with terms and conditions specified by the software licensor.
Software Licensee	A legal entity, typically a person or organization, contractually bound to a given software license agreement that provides rights to use the associated software in accordance with the terms and conditions as specified by the copyright owner.
Software Vendor, Independent Software Vendor (ISV), Application Producer	The software vendor is a party that owns the copyright in the software or licenses the software.
Workload	A machine image or virtual machine instance and information on the technical layout (such as the number of cores and amount of RAM), network configuration, and the data store directly associated with the virtual machine (VM). The VM is the abstraction of all the workload's constituent elements.
Entitlement Usage Metrics	Entitlement usage metrics are generated from events that measure the use of a software product instance. Entitlement usage metrics may be gathered on the consumption of a licensed software product instance.
Asset Manager	Roles within an organization responsible for the proper management of the IT assets (applications, systems, technical and business services).
License Auditor	Roles within or external to an organization responsible for the independent audit of software licensing usage patterns.
Infrastructure Architect	Roles within an organization responsible for developing infrastructure and platform architecture.
Procurement Manager	Roles within an organization responsible for purchasing, procurement, negotiations, and commercials.
Software License Optimization Vendor	Solution providers and vendors that provide applications and solutions to optimize the value of software licenses.
Legal Advisor	Legal specialists or professionals providing advice on software licensing matters.

SOFTWARE LICENSING ISSUES, CHALLENGES, AND OPPORTUNITIES

Software Licensing Models

Licensing models and schemes currently in use in the industry range from models suitable for traditional IT deployments (for example, in-house and enterprise data centers) to models suitable for cloud deployments (true variable and consumption- and capacity-based pricing). Leading ISVs have created new licensing models or adjusted existing ones to provide additional flexibility. Appendix 1: Licensing Models lists examples of various licensing models offered by software vendors.

Emerging cloud-based licensing models include:

- **SaaS context.** Pay-as-you-go or subscription-based licenses are often applied to software used in the cloud. For example, several SaaS implementations are licensed according to the number of users, on a subscription basis. This model simplifies the software licensing implications for cloud subscribers—the SaaS provider assumes primary accountability for managing the licensing of underlying software components that are not developed and owned by the SaaS provider (for example, the operating system, database, middleware, and so on). The service consumer is accountable for auditing and monitoring compliance with the terms of service of the SaaS solution.

- **IaaS and PaaS context.** Within infrastructure as a service (IaaS) or PaaS environments, complexities arise when moving existing IT system and associated licenses from enterprise data centers to the cloud. The challenges are largely due to issues involving licensing model restrictions and differences, commercial restrictions, and constraints inherent in licensing agreements. Traditional license models are now available in the cloud through licenses already owned by enterprises. New pay-as-you-go and subscription models are attractive for new services, IaaS, and other offerings to accommodate the flexibility needed by both cloud providers and cloud subscribers and to minimize risks.

- **Platform-based context limitations.** Licenses locked to physical infrastructure limit the ability to move workloads and take advantage of underlying compute power without additional negotiation with the software vendor. Hardware platform or device-based models are not suitable for the cloud environment, and others may be difficult to administer, too.

Issues that Software Consumers and ISVs Face

Perceptions often drive expectations, creating a gap between what software consumers think is a fair price and what ISVs think they deserve for their solution. This factor has contributed to the diversity of software licensing and pricing models being demanded by enterprises and offered by application producers.

Software vendors invest in diverse licensing approaches to:

- Increase the predictability of software revenue
- Understand more clearly how customers are using software products and maintenance offerings; this helps determine the value proposition for the customer and, consequently, to more accurately reflect these values and understanding of the customer needs when pricing solutions
- Demonstrate the value of software as part of a broader solution

Software customers expect software vendors to:

- Improve the effectiveness of current licensing practices
- Place greater focus on understanding customer business needs
- Offer greater flexibility and simplicity when structuring software licensing contracts

Note: Considering the pervasive nature of cloud, if this list of objectives can be attained, ISVs stand to increase consumption. Cloud consumers will access the services through more diverse channels and devices, and use the technology more effectively; this in turn increases the perceived value of the system, likely resulting in a sizable increase in the user base.

Common Ground: Software Consumers and ISVs

Software consumers and ISVs share a great deal of common ground when facing the current set of challenges. Motivations to resolve the challenges stem from the following three traits.

- **Increased predictability.** Software vendors are expecting predictability of software licensing and maintenance revenue streams. Software consumers are expecting predictability of the investment and costs incurred through software licensing.

- **Decreased complexity.** Complexity and noncompliance are linked. Both ISVs and consumers favor simplicity, to support effective sales cycles, negotiations, compliance, and value generation.

- **Improved alignment with value.** Both software vendors and software consumers benefit by resolving the price-value disconnect for software. Demonstrating the tangible value of software through business proof points and metrics can provide alignment in the perception of value and quantitative evidence to support this point.

"Application producers currently offer a wide variety of software pricing models, which reflects a great diversity in demand for how enterprises want to consume software. Node locked (40 percent) and feature concurrent user (floating or network license) (39 percent) are the most prevalent pricing models. Device (33 percent), named-user (27 percent), token concurrent user (floating or network license) (24 percent), site (22 percent) and client access license (CAL) (21 percent) are also popular. Looking out over the next 18 to 24 months, feature concurrent user (floating or network license) and node locked licensing are expected to remain the most prevalent. However utility model (usage, time, number of transactions) is expected to grow by 23 percent, further signaling increased interest in usage-based pricing."[2]

By diversifying and enhancing their licensing models and pricing strategies, ISVs can balance revenue optimization with customer satisfaction. This takes the form of consumption-based software licensing models (sometimes called *utility models*), driving licensing costs through usage, time, the number of transactions, capacity, and so on.

REQUIREMENTS FOR EFFECTIVE MANAGEMENT OF SOFTWARE ENTITLEMENTS

The ODCA recommends the following requirements to support the effective management of software entitlements and generate increased business value from software investment within cloud deployments. The Alliance believes that selective content from this section should be included in requests for proposal (RFPs) to cloud providers to ensure that proposed services support the Software Entitlement Management Framework. For further details, please refer to RFP Requirements. Requirements from this section should also be used to support commercial, strategic, and operational dialogue between software consumers (including cloud providers and cloud subscribers) and software providers (including software vendors, ISVs, and application producers).

Software Vendor Relationship Management

The cloud subscriber and cloud provider should develop and maintain a strong relationship with representatives from the respective software vendors.

This requirement enables a cloud subscriber and cloud provider to readily contact software vendor representatives with software queries, including the procurement of new licenses or amendment of existing licenses, and creates a direct link with the software vendor. This also enables the ISV to further business relationships and better understand customer needs and value proposition.

Software Procurement Policy

The cloud subscriber and cloud provider enterprise should develop, publish, and manage an internal software procurement policy. The software procurement policy should establish clear guidelines in relation to:

- What team or role capacity from within the cloud subscriber enterprise can procure software products on behalf of the enterprise? For example, can employees procure software products directly by means of Internet download and acceptance of click-through terms?

- Where is the software deployment authorized and who within the software user (customer) enterprise can authorize redeployment or migration to a new environment?

- What are the enterprise-approved commercial considerations in relation to licensing metrics? For example, would a concurrent user license be more cost effective than a named user license? What is the role of legal representatives to assist with contract negotiations?

- Which team is responsible for supporting and managing license rights and compliance with license obligations?

- How will software license fees be paid and through which payment channels?

- What is the process for retiring old applications or products that are no longer required or used by the cloud subscriber? This includes consolidation of software licenses.

---

[2] The "2012 Key Trends in Software Pricing and Licensing" survey was conducted by Flexera Software with input from IDC's Software Pricing and Licensing Research division.
http://learn.flexerasoftware.com/content/ECM-WP-Software-Licensing-Pricing-Report

- Where does the responsibility reside for cloud service provider-based licenses, and who oversees the adoption or extension of those for use in the enterprise?
- What is the enterprise perspective on user acceptance of license condition acceptance through disclaimers that form part of the cloud service ordering process (within the cloud ordering portal)?

Creating and publishing a software procurement policy for use by cloud subscriber employees and cloud provider staff provides the capability for centralized procurement and management function for all software products. It also reduces risk exposure by eliminating the acceptance of unfavorable contractual terms, impracticable and unmanageable license usage rights and restrictions, and inappropriate financial costs.

Software Library

The cloud subscriber should implement a software library to catalog all third-party software products that are currently being licensed by the cloud subscriber. Key attributes of the software library typically include:

- Identification of the third-party software vendor
- Term of the license
- Licensing metrics and model used, such as named user, concurrent license, volume license, enterprise license, evaluation license, trial license, original equipment manufacturers, hardware platform- or device-based, role-based, employee-based, financial-based, or transaction-based
- Usage rights and restrictions
- License deployments to identify exactly where the third-party software licenses have been deployed by the cloud subscriber; for example, location, installation date, machine/infrastructure, or user
- Deployment restrictions, including geographical restrictions
- Termination provisions, including post-termination transition rights

By developing and maintaining a software library catalog, the cloud subscriber can easily identify and access information about its third-party software licenses and support the analysis of migrating applications to the cloud.

Understand License Restrictions

Before starting any engagement with a cloud provider, cloud subscribers should conduct an audit of its existing third-party software licenses to fully understand license restrictions and to determine whether the existing software license model permits the migration of the software to the cloud. The audit should be supported by a software library or asset inventory.

The following considerations should be an integral part of the audit process to understand license restrictions.

- Identify the software products to be included in the migration to the cloud, listing all software products against attributes such as third-party vendor and software licensee (in some cases, software licenses may be managed by parent companies on behalf of their affiliates or particular business units within larger corporations).
- Locate the corresponding license agreements for the software products.
- Consult with the cloud provider to determine how the software entitlement will be deployed across the physical and/or virtual infrastructure by the cloud provider.
- Assess the number of cloud subscriber users who will be allowed access to the software on the cloud.
- Assess the location or region where the software will be stored.
- Assess whether any part of the cloud services delivered by the cloud provider is outsourced or subcontracted to any other third parties.
- Assess the license rights and restrictions, and other constraints that apply. This includes, but is not limited to:
  – Is migration to the cloud permitted?
  – Is the license grant subject to deployment to, and access from, a defined location or region?
  – Will the third-party software vendor offer support for the software product if used from the cloud?
  – Does the license grant allow for transitory use of the software product?
  – What additional restrictions will the third-party software vendor seek to impose on the license?
  – Consult with the cloud provider on how the tracking, monitoring, measurement, and reporting of the license consumption will be performed. Also, determine the data and metadata that will be shared and the formats in which this data will be provided.

Analyze the Cloud Providers

The cloud subscriber should research and analyze the cloud provider's products and service offerings, and contractual terms to identify and understand the cloud's infrastructure capabilities, such as virtualization and elasticity, and limitations imposed by existing software entitlements with third-party software vendors.

The essential capabilities that cloud subscribers should look for when identifying their cloud provider of choice are:

- Services and features to simplify the management and monitoring of software entitlements at a consumer level, including support of software asset management requirements
- Maintenance of the deployment inventory
- Time-based reporting of software deployments
- Report on contents of operating system instances
- Techniques used within the infrastructure to manage elasticity according to the entitlement limits

The analysis of cloud provider capabilities enables the cloud subscriber to select a cloud provider closely aligned with its functional requirements and specifications and equally aligned in terms of software license restrictions. The "ODCA Master Usage Model: Commercial Framework"[3] document provides a framework for commercial contracts and master service agreements between cloud subscribers and cloud providers.

Review Licensing Agreements and Contracts

The software user (cloud subscriber and cloud provider) should assess and review the licensing agreements and contracts between key stakeholders to analyze whether they meet business needs and obligations (for example, the financial, legal, and compliance obligations).

- The cloud subscriber should assess the commercial goals of the cloud arrangement and pricing models (whether fixed or variable), evaluating the anticipated workloads for normal and above-normal business patterns from a short-term and long-term perspective. The cloud subscriber should review which type of licensing model(s) are more effective to meet their needs based on usage patterns envisioned.
- Interoperability. Software entitlement models should include support for the cloud subscribers' capabilities to do business with interoperable cloud services across alternate service providers.
- Commitments. The cloud subscriber should analyze whether the software entitlement management schemes require minimum purchase volumes or multiyear commitments; this may impede the flexibility to scale up and down to accommodate varying levels of business operations.
- Existing contractual rights, restrictions and obligations, and amendments that may be required to the license agreement to facilitate the software migration to the cloud should be considered. Typically, this involves contract reviews between the consumer (cloud subscriber) and the software licensor (ISV), consumer (cloud subscriber) and provider (cloud provider), and provider (cloud provider) and software licensor (ISV).
- The implications of any open-source software being used by the cloud provider to deliver the contracted services and the implications of entitlements to upgrades and new releases from the third-party software provider should be clearly assessed and well controlled.
- The cloud subscriber (and the cloud provider) should determine the licensing options for the third-party software vendors to identify whether they offer cloud-based licensing models that meet the business needs and usage patterns of the software consumer.
- The definition of the "Licensee" bears importance for both financial and legal reasons. To maintain financial controls, the licensor might want to restrict the definition of licensee.
- When assessing licensing implications, determine whether installing the software on cloud provider's platform is considered "use" of the licensed software by a third party, or considered "assignment" of the license to another entity.
- Some software entitlements place restrictions on the software licensee in terms of how the licensed software may be used. Analyze whether the restrictions on use have been considered, understood, and assessed for cloud arrangements.
- Some software entitlements place restrictions on the licensee, limiting where the licensed software may be used (such as class of machine, CPU, vendor platform, and platform type). Analyze whether the restrictions on use have been assessed and understood for cloud arrangements. For example, review the product use rights tied to virtualization or specific vendor rules for cloud-computing environments.
- Consider the period of notice required to terminate the software entitlements and any fees that apply for early termination or termination without notice.

---

[3] www.opendatacenteralliance.org/docs/ODCA_Commercial_Framework_MasterUM_v1.0_Nov2012.pdf

- The cloud subscriber should analyze whether the commercial framework and master services agreement between the parties (cloud subscriber and the cloud provider) should incorporate any requirements and implications arising out of third-party software vendor license requirements and obligations.
- The cloud subscriber should determine the flexibility offered by the software licensing models within the licensing contracts and agreements to support changes to their business model, mergers, acquisitions, geographical boundary changes, business growth, business downsizing, and other variances.

Geographical and Location-based Requirements

Some software entitlements restrict where the software can be deployed or used, as stated by the vendor or government agency. Ensuring that the restrictions on geographical locations where a license can be used is important to meet commercial and regulatory obligations.

- The cloud subscriber should identify and contractually manage the geographical locations from which the services will be provisioned and offered by the cloud provider.
- Software access rights should be clearly defined and managed in the context of user types, business need, and location of access.
- The implications of provision of cloud services, including administration of IT systems, infrastructure, and help desk support, from embargoed countries should be well understood and contractually controlled. Internet-based access makes user location tougher to track and could breach export laws, regulatory mandates, or enterprise policies.
- The impact of routine maintenance performance by cloud providers should be assessed and managed.

Mobility and Migration

- Software licensing models should support the ability to move applications and data from one virtualized environment to another, including:
  - Physical enterprise data centers to virtual data centers
  - A virtual host to another virtual host within a virtual data center
  - One host to another host within a public cloud
  - One host to another host within a private cloud
  - A virtual data center to a public cloud, and back
  - A private cloud to a public cloud, and back
  - A public cloud to another public cloud, and back
- The cloud subscriber should plan software migration and implement internal controls to monitor the migration of the software products to the cloud. Migrations should allow sufficient time to facilitate cost-effective and timely redeployment and migration of the software and entitlements to the cloud. Key requirements are:
  - Identify and resolve redeployment and migration restrictions associated with the software license.
  - Gain a clear understanding of contractual terms used within the software license scope (for example, does "processor" mean CPU or core? Does "named user" include or exclude batch processing?).
  - Engage legal advisers to negotiate with the third-party software vendor for the purpose of amending existing software license agreements (where required) and cloud provider agreements.
  - Determine what software licenses can support cloud bursting or migrating from one cloud to another.
- Movement of cloud services and workloads (to balance the data center load, support disaster recovery, handle data center migrations, handle capacity burst requirements, provide price-sensitive services, and so on) is quite common; this results in moving software entitlements across different infrastructure and physical data center locations.
  - The cloud subscriber and the cloud provider should ensure that movement of workloads does not breach privacy obligations, export regulations, commercial obligations and license restrictions of the software licensor, and operational service levels.
  - Adequate measures should be in place to control and track software deployments in support of migration operations (standby equipment to contend with hardware failure, parallel maintenance tasks to facilitate workload shifting, load balancing to ensure stable service quality). Failure to adequately control and track software deployments exposes the cloud subscriber to a possible breach of the software-entitlement obligations. In a worst-case scenario, this could represent a violation of regulatory mandates.
- Cloning of virtual machines: Inadvertent cloning of virtual machines and corresponding applications could create software license violations, as well as possible security compliance risks. The cloud subscriber should prevent unauthorized cloning of protected assets across clouds, as well as ensure that the cloud provider does not do so.

Elasticity

- The implications of elasticity on licensing quotas and burst requirements should be assessed and controlled.

- Design. The cloud provider should design an elastic infrastructure with defined limits that will ensure software entitlement obligations are maintained and also map a cloud deployment back to the associated software entitlements.

Traceability

The characteristics of licensed software product instances and the consumption of them should be traceable regardless of the environment in which the product is deployed (physical or virtual computing through a virtualized environment, from the cloud and through an enterprise data center).

- The properties traced should include:
  - The identification of each software instance and where it is deployed
  - Whether the software is in current use
  - The ability to map a cloud deployment back to its corresponding software entitlements
  - Provisions for accommodating "legacy" software entitlement agreements, such as those that correspond to physical-hardware deployment.

- The characteristics of a licensed software product should be captured in a computable package, such as an Open Virtualization Format (OVF) package. OVF 1.1 is a Distributed Management Task Force (DMTF) Standard and recently was approved as an ISO/IEC International Standard. OVF is a standard format for packaging virtual appliances or machines. This allows the virtual machine to be more easily moved and deployed across virtualization platforms.

Packaging and Deployment

Licensed software products can be packaged to form solutions, suites, bundles, and virtual appliances.

- The software vendor should provide standard and interoperable capabilities to discover the software products bundled within the deployment package and use this information for automation and management of software installation, auditing, and removal.

Measurement and Analysis of Entitlements

The cloud subscriber should implement processes and tools to uniquely identify and track usage for any instance of a licensed software product. Measurement and analysis of entitlements should allow a cloud subscriber to monitor software use compliance, assess licensing requirements, and reduce license fee costs.

- The cloud subscriber should monitor license compliance and implement controls to manage licensing compliance breaches.

- For accounting and legal compliance, customers (cloud subscribers) should keep a record of their software entitlements and software usage. A cloud environment adds complexities to this recordkeeping, because of the interdependent operational processes involved in delivery of cloud services.

- The cloud subscriber and the cloud provider should use software asset management processes and tools to support the tracking, monitoring, and optimization of software licensing investments across enterprise data centers and cloud deployments (internal or external).

- License compliance software - the cloud subscriber and the cloud provider should deploy license compliance software to determine license breaches and usage limitations.

- The cloud subscriber and the cloud provider should clearly agree and determine who is responsible if software users exceed their entitlements during any stage of the cloud lifecycle operations. This is a significant consideration, as the cloud provider may or may not be in a position to indicate software entitlement breaches to the cloud subscriber. If the cloud provider is not to be held liable, they may require some form of indemnity from the cloud subscriber to that effect.

- The cloud subscriber should analyze whether the cloud provider has appropriate reporting capability that will support the cloud subscriber's need to audit software entitlement compliance, including the capability to audit, evaluate, and report on the cloud subscriber's software entitlement to the third-party software provider(s).

- Metrics - the cloud subscriber, cloud provider, and the software vendor should agree on common metrics to support the true measurement of exactly what is consumed. The metrics should be supported by ODCA Standard Units of Measure, as well as industry standards, to enable comparison of software entitlement costs and benefits. ODCA recommends that a standard and common data model should be developed for monitoring, metering, and auditing of software entitlements. The standard data model will facilitate widespread adoption by cloud providers and cloud subscribers, and enable cloud subscribers to access compliant and commercially viable services and solutions for software entitlement management.

- The cloud subscriber should undertake an assessment of software entitlements pertaining to use (overuse or under use) of entitlements. Software licenses that are no longer in use should be retired or allocated to another user. If certain software products are being overused and this is evident in the reports, a new volume licensing regime could be more cost effective for the cloud provider or cloud subscriber.

Roles and Responsibilities for Service Consumption and Billing

The metering and monitoring processes for cloud services should be well defined, including outlining the following:

- Roles and responsibilities for metering, monitoring, and dispute management
- The role of capabilities, such as the configuration management database (CMDB), to determine service consumption and billing in regard to software entitlement management
- The method for software entitlement management billing, including frequency, billing cycle, payment terms, methodology to support the correct cost triggers, and penalties for non-payment or late payment, including the impact on services provisioned, impact of workload migration, and bursting against base software entitlement

Requirements Summary

It should be noted that cloud subscribers could procure licenses for deployment within their internal in-house environment, deployment within the cloud provider's environment, or they could also use software from the cloud provider that includes software licenses incorporated within the service. The requirements for software entitlement management are therefore applicable to both cloud subscribers and cloud providers, in their role as provider of software licenses incorporated within a service, such as Service Provider License Agreements (SPLAs).

RFP REQUIREMENTS

The following are requirements that the Alliance believes should be included in RFPs to cloud providers to ensure that proposed services support the Software Entitlement Management Framework. Because the level of responsibility for software entitlement management changes depending on the cloud deployment model and how services are offered, the following RFP questions are documented as "should" rather than "must."

- The cloud provider should provide services and features to simplify the management and monitoring of software entitlements at a consumer level, including support of software asset management requirements.
- The cloud provider should provide the capability to report on deployment inventory, software deployments, and contents of operating system instances.
- The cloud provider should provide contractual clarity on the location of provisioned cloud services, including administration of IT systems, infrastructure, and help desk support.
- The cloud provider should ensure that movement of workloads does not breach privacy obligations, export regulations, commercial obligations and license restrictions of the software licensor, and operational service levels.
- Adequate measures should be in place to control and track software deployments in support of migration operations. These measures include standby equipment to contend with hardware failure, parallel maintenance tasks to facilitate workload shifting, and load balancing to ensure stable service quality.
- The cloud provider should design an elastic infrastructure with defined limits that will ensure software entitlement obligations are maintained.
- The characteristics of licensed software product instances and the consumption of them should be traceable, regardless of the environment in which the product is deployed.
- The cloud provider should monitor license compliance and implement controls to manage licensing compliance breaches.
- The cloud provider should use software asset management processes and tools to support the tracking, monitoring, and optimization of software licensing investments.

- The cloud subscriber and the cloud provider should clearly agree and determine who is responsible if software users exceed their entitlements during any stage of the cloud lifecycle operations.
- The cloud provider should possess appropriate reporting capability to support the need to audit, evaluate, and report on software entitlement compliance.
- The cloud subscriber should provide the metrics to support the true measurement of service consumption and software usage.
- The cloud provider should provide metering and monitoring processes for cloud services, with a focus on roles and responsibilities for metering, monitoring, and dispute management.
- The cloud provider should provide capabilities to support the determination of service consumption and billing in regard to software entitlement management.
- The cloud provider should provide clarity on the impact of workload migration and cloud bursting on software entitlement.

PROCESS FLOWS

Software Entitlement Management Process Flow

The integration of software entitlement management and its implications across the cloud lifecycle are illustrated in Figure 1. Once a commercial contract (master services agreement) has been set up with a cloud provider, the cloud arrangement is controlled through a set of key operational processes and lifecycle steps. The processes take place between the customers and users, and the suppliers and providers, as shown above and below respectively in the figure. Each group has its own set of interactions, illustrated with arrows communicating with the central entity. The processes, described from left to right, follow a logical sequence, although some of them are invoked iteratively, and in some cases there are more complex patterns involved between processes.

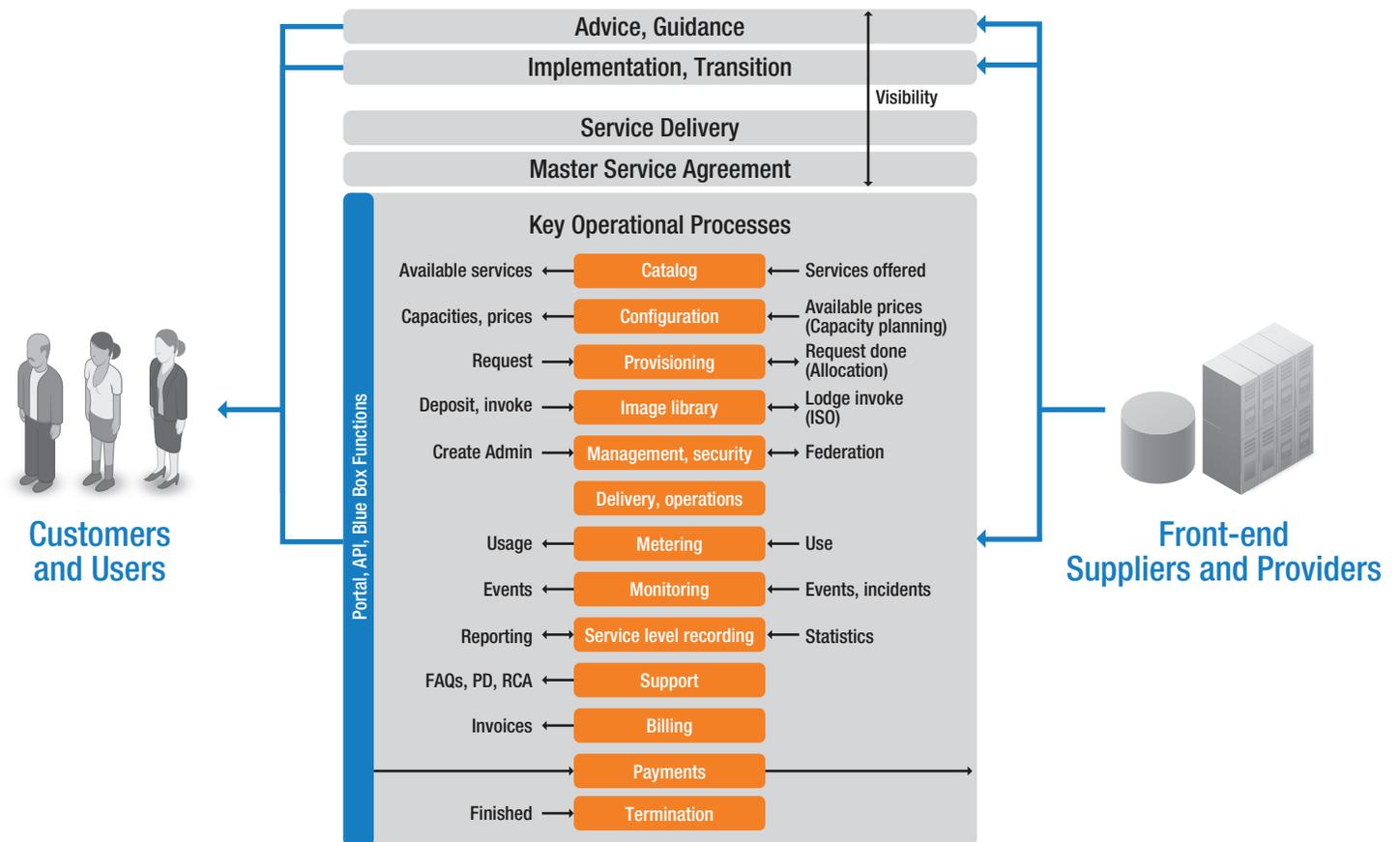Table 3 provides additional information about each process shown in the figure.

Figure 1. The integration of software entitlement management and its implications across the cloud lifecycle.

Table 3. The software entitlement management process flow consists of key operational processes.

Process	Activity	Supplier Interaction	Customer Interaction	Software Entitlement Impact
Catalog	Maintain a superset catalog of available services and levels.	Provide structured information on what is generally available.	Query the catalog(s) for available services.	The services could include the use of proprietary software that requires licensing. Some independent software vendors (ISVs) have special arrangements for this (for example, the Microsoft Services Provider License Agreement arrangement).
Configuration	Maintain a CMBD to define what is available in real time and applicable prices.	Update with current configuration and prices (for example, including spot prices).	Extract available capacities and prices.	Not applicable.
Provisioning	Assign required workload to available environment(s), based on given criteria.	Fulfill allocation requests.	Issue request, including possible supplier(s) preference.	Library: can potentially invoke images that have embedded software, in which case the records need updating appropriately.
Image Library	Maintain and invoke a library of virtual machine images with pre-installed software.	Lodge images in library, cache/download and invoke them on request.	Deposit images, request their invocation.	
Identity Management	Employ federated identity management for SSO and other uses (for example, based on SAML).	Request authorization checks.	Provide access to maintained identity sources.	Could include information required for user-based software licensing.
Delivery and Operations	Deliver and use the ongoing operational services, including installing and using software.	Suppliers provide ongoing environment.	Users make use of environment(s).	Could involve the installation of software, if not part of a pre-configured image and its use. These events can cause the updating of a software entitlement database.
Metering	Register actual use of service components, in given units.	Provide records of resource usage.	Extract records of usage, where required.	Could involve recording the use of software or simply of resources to which software usage is associated, such as CPU cycles or transactions.
Monitoring	Detect and forward system events (for example, failures) and invoke reconfiguration when appropriate.	Forward events and alerts.	Accept own events for processing, if required.	Not applicable.
Service-level Recording	Maintain a record of actual service levels delivered.	Provide records and statistics on actual service levels delivered.	Access service-level reports for monitoring, as required.	Not applicable.
Support	Optionally, provide support and assistance in problem analysis and solving for the environment, including software (for example, root cause analysis, bypasses, and so on).	Provide support information: hardware and software levels, configuration, and so on.	Assist in root cause analysis (RCA) and problem determination (PD). Access FAQs, where needed.	Could require the use of special access to the software, to perform problem tracing or fulfill technical support needs.
Billing	Arrange payment for resource usage, including software as appropriate.	Provide information, from Catalog, Configuration, and Metering.	Accept invoices.	Could involve charging for software, either on the part of the supplier or a third-party ISV, if the software is so provided.
Payments	Arrange payment of the invoices for resources, possibly including software.	Accept and ascribe payments.	Make payments.	As per Billing, can include payments due to an ISV.
Termination	Terminate services and charges, when no longer required.	Terminate underlying service resources, remove data and software.	Request termination, update records.	For usage-based licensing, should register the cessation of software usage.

During Delivery and Operations, other activities can be triggered by internal or external events, such as load-balancing or bursting to other cloud environments.

The horizontal arrows shown in the figure indicate that there could be interactions between the processes. This might not be exhaustive, as the whole environment is flexible and responsive to events.

- Provisioning, or re-provisioning, can be triggered by other events, such as service levels not being met or being exceeded, or termination of some facilities.
- Billing is triggered by Catalog, Configuration, and Metering.
- Support may be triggered by Metering, Monitoring, and Service Level Recording.

These processes are surrounded by other services and provisions, as further shown, many or all of which can in turn have software entitlement implications.

- Suppliers can offer advice and guidance as to how services might be used or configured. This can encompass their own services, as well as those from other providers when acting as a value-added reseller.
- Suppliers can assist in the implementation of the service components and transition of the customer's systems to those environments.
- A Master Services Agreement, as defined by the ODCA, may be formulated between the supplier(s) and customer(s).
- If there is a central clearing or brokerage function, how much of the information and transactions should reasonably be visible to the other parties involved.
  - Can a supplier see the other suppliers' available configurations and prices?
  - Can a customer see who else has been obtaining specific services and for how much?

As well as commercial confidence, issues around cartel formation can arise if proper protections are not put in place.

USE CASES

Software licensing use cases, as considered from the cloud lifecycle perspective, can be distilled to three broad cases.

- Software installation and removal
- Software activation and de-activation
- Measurement and reporting of software use

Usage Scenario: Install and Uninstall Software in the Cloud

Description

This use case enables a cloud subscriber to install software into the cloud. The deployment can be on a virtual or physical infrastructure, depending on the specific infrastructure requirements of the cloud subscriber. When no longer needed or licensed, the cloud subscriber then uninstalls the software from the virtual and physical environments.

Technically, these steps might involve just deploying a script to install the software (bundle) or remove it, but the steps need to align with the license conditions agreed to by the cloud subscriber, ISV, and possibly the cloud provider, who usually requires the subscriber to ensure compliance with all applicable licenses. Aspects that should be addressed:

- Who is the owner or who is expected to pay how much?
- What type of license is involved?
- What are the limitations on license transferability?
- What does the license span include; for example, specific CPUs, servers, clusters, data centers, and geographies?
- Is there a mechanism for evidence and usage-reporting criteria?

Preconditions

The cloud subscriber has the necessary software deployment and software removal access to the infrastructure and the ability to check for available licenses or a method for obtaining new licenses.

Post-conditions

The software deployment register is updated with the details of deployment. This information includes the following:

- What was installed
- Where it is installed
- The configuration of what it was installed on
- What was uninstalled
- Where it was uninstalled from
- The license count before and after installation and removal
- Evidence and usage reporting is in place
- The installed software is available to be configured for use according to the cloud subscriber's requirements
- Billing is in place

Primary actor

Cloud subscriber

Secondary actors

Cloud provider, ISV

Usage Scenario: Software Activation, De-activation, and License Float

Description

This use case enables a cloud subscriber to activate and de-activate software licenses, as needed. This could be accomplished by enabling a certain number of licenses for consumption or by activating servers (real or virtual), each with a certain number of licenses associated with it. The same operation can be done in reverse, to de-activate servers and de-activate a portion of licenses.

This use case also enables a cloud provider to dynamically activate resources (including servers and licenses), float licenses to balance the load over data centers as part of behavioral analysis service management, optimize performance, or ensure service availability in case of a data center outage.

Technically, dynamic activation and license float might consist of only deploying a script to "turn on" additional servers with pre-loaded software or to move the software (bundle) from one to another location, but implications on license usage should be clear from a usage compliance perspective. License activation and float need to be in alignment with the license conditions agreed to by the cloud subscriber, ISV, and possibly the cloud provider, who often requires the subscriber to ensure compliance with all applicable licenses. The following aspects need to be considered:

- License span, including, for example, specific CPUs, servers, clusters, data centers, and geographies; this also includes compliance with government regulations
- Who should be paid; for example, the local vendor representative
- Evidence and usage reporting criteria
- When increasing the allocated processing allocation, the use case should ensure the license entitlement is not exceeded
- When decreasing the processing allocation, the use case should ensure the minimum processing capacity requirements are not breached

Preconditions

Software entitlement rules describe granularity of license activation; for example, one-by-one, hundreds at a time, or thousands at a time.

Software entitlement rules enable the migration to be performed.

Post-conditions

The software deployment register is updated with the number of active and inactive licenses, the time stamp of activation and deactivation, as well as license use details such as location and server ID. This register should maintain a log of all activations and deactivations for a specified period of time.

The OSI is moved to virtual infrastructure that complies with the cloud subscriber's software entitlements.

Billing and payment are adjusted.

Primary actors
Cloud subscriber and cloud provider

Secondary actor
ISV

Usage Scenario: Measurement, Audit, and Reporting of Software Use

Description

This use case enables the cloud subscriber to access the software deployment register to review, audit, and report what software has been installed, uninstalled, activated, deactivated, and moved in the cloud. The register provides details about each license, including assignment to a server (physical and virtual), cluster, data center, and geography, and the duration of such assignments.

Information provided by the register can help in compliance and auditing of license agreements. It can also help the cloud subscriber to more accurately measure the number and duration of license uses, which can lead to optimal budgeting for a maximum number of licenses they need. The information also enables the ISVs to ensure they are getting paid for the licenses they delivered.

If cloud subscribers are providing certain kinds (for example, OS-level) or amounts of licenses, they can also benefit from using the register to monitor, optimize, and report on the license use.

Preconditions

The software deployment register logs include information about the license installation, removal, activation, deactivation, movement, and duration of use.

Post-conditions

The software deployment register is up to date. If an audit report was completed, it is recorded.

Primary actor
Cloud subscriber

Secondary actors
Cloud provider, software vendor

ODCA WORKING TOGETHER WITH DMTF

With cloud computing becoming mainstream, a number of emerging usage models—such as workload migration and being able to dial up and down capacity on the fly—have become very desirable. While these types of usages provide a great deal flexibility and elasticity, they also create a number of challenges in management of software license entitlement. Cloud providers and cloud subscribers are often uncertain about the state of compliance to software entitlement, including concerns such as inefficiencies, associated risks, and complexities in managing software entitlement. In the absence of standards and good practices (shown in Figure 2), it will be left to cloud providers to implement customized solutions for software entitlement management that may increase management complexity for the cloud provider, as well as increase cloud provider and solution provider lock-in for cloud subscribers.

The ODCA and DMTF share these common concerns and have announced plans to work together to resolve significant software entitlement challenges hindering cloud adoption through the synthesis of enterprise customer requirements, usage models, recommendations, and standardization of software entitlement practices. The two organizations plan to collaborate through joint work products, working group representation, and development of complementary insights designed to resolve software entitlement management challenges and encourage standard and interoperable solutions.

Figure 2 illustrates the proposed ODCA and DMTF collaborative effort to address industry challenges with software identification and entitlement management.
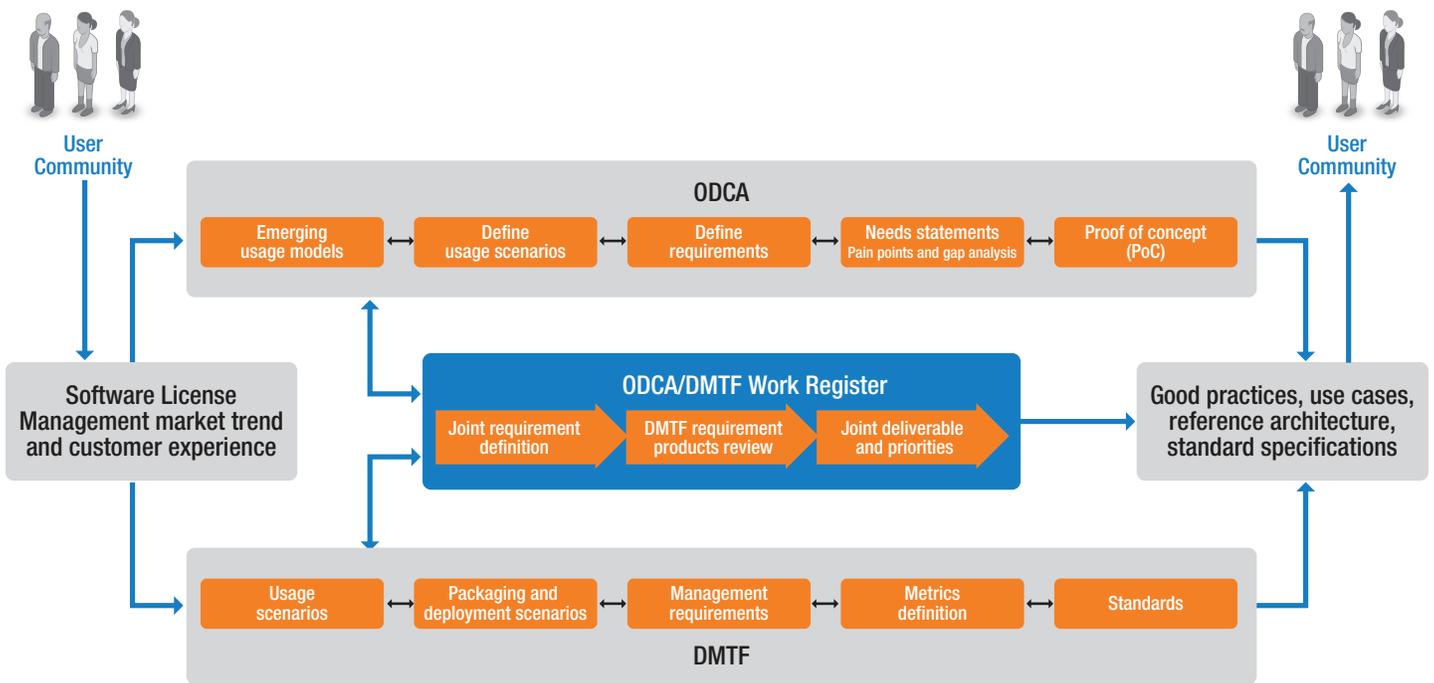

Figure 2. The Open Data Center Alliance and Distributed Management Task Force have announced plans to work together to address industry challenges with software identification and entitlement management.

To manage licensed software product(s) and product usage, DMTF is working on these issues:

- Recording and enumerating software product usage. This potentially encompasses the instances, customers, users, CPUs, or other measurable units that may be running, where they are running (such as, whether in an operating system on a hardware server, or a virtualized or cloud computing environment), with what device, and by whom (that is, on which processor of a given hardware server).
- Uniquely identifying the software licensed product(s) associated with a particular usage.
- Technically conveying product usage information of licensed product(s) for pre-deployment or reporting purposes. For example, this could include software entitlement metrics requirements in a package such as Open Virtualization Format (OVF).

This is further described in the white paper published by the DMTF in 2012, which defines a set of desired standards (DSP-IS0301) that enables the cloud subscriber to effectively manage software inventory and deployment configuration in a private or public cloud environment.[4] One intended usage of these standards is that the product identity and the core metric requirements can be carried in an OVF package for use by an automated deployment system or as part of a private or public cloud deployment package.

The use of metadata models for software entitlement management auditing in a heterogonous and mixed implementation environment (typical within cloud providers) will lead to easier auditability, as well as implementation processes for monitoring and accounting.

The ODCA sees the DMTF deliverables as enabling the ODCA's Software Entitlement Management Framework requirements and bringing consistency and completeness to implementation models and processes. Key processes such as discovery of software usage integrated in virtualization engines and cloud environments, interrogation of installed images, and related tasks can be supported through the standards being developed by DMTF. These standards also reduce the intrusiveness caused by software auditing tasks and processes.

OTHER SOURCES OF SOFTWARE ASSET MANAGEMENT INFORMATION

During the production of this document, members of the ODCA became aware of a number of other organizations that are working in this area. Most of their work appears to be focused on the supply-side mechanisms or software-asset-and-use tracking, instead of the user's business requirements perspective, which is the focus of this document.

Most notable is the ISO/IEC 19770 standards, being developed by the ISO/IEC JTC1 SCY Working Group 21 (WG21), whose work can be found at www.19770.org. This group identifies the following relevant standards developments:

- 19770-5 – The overview standard
- 19770-1 – Process standards
- 19770-2 – Software identification tags: an XML-based structure with the metadata to manage installed software
- 19770-3 – Software entitlement tags: an XML-format encapsulation of a customer's licensing rights and limitations
- 19770-7 – Tag management processes and guidelines

In addition, TagVault.org is a non-profit organization, formed under the structure of IEEE-ISTO as a registration and certification authority for software identification tags (SWID tags) based on the ISO/IEC 19770-2:2009 standard.

In February 2008, a 30-month project called SmartLM was initiated under the sponsorship of the European Commission FP7 funding program. The results, including a white paper, can be found at www.smartlm.eu.

---

[4] Distributed Management Task Force: "Software Identification and Entitlement Usage Metrics" white paper (DSP-IS0301).

RECOMMENDATIONS AND INDUSTRY ACTIONS REQUIRED

The ODCA proposes the following recommendations and further industry actions to improve the effectiveness of software entitlement management in cloud deployments.

Cloud subscribers need to able to run their application services across different cloud platforms using different providers without breaching licensing rules, incurring penalties, or being impacted by unpredictable events and outcomes. In other words, the consumer needs predictability regarding software consumption costs that is not dependent on the underlying technology platform, such as the capacity of the entire server farm). They also need facilities to be aware of their levels of software usage and how they compare to their entitlements, across multiple software providers and multiple cloud and hybrid environments. Cloud subscribers should ally with the cloud providers and standards bodies to encourage adoption and use of standardized software entitlement management tools.

Cloud providers should favor and use standardized software entitlement management tools. They should collaborate with the cloud subscribers to insist on such tools.

Software vendors should adapt their licensing models to make them relevant in a cloud environment. These ISVs should actively consider real-time consumption models and software entitlement management models to support cloud subscribers in improving the flexibility in utilizing whatever software their business needs, at an affordable price and with minimal administrative overhead.

Those consumption models should be aligned to the units defined in the Usage document "Standard Units of Measurement for IaaS,"[5] so that software usage can easily be aligned to scales of environment, for any software thus licensed.

They should contribute to and implement standards for entitlement tracking, both data models and usage protocols, so that subscribers can achieve visibility of their usage, not only across multiple clouds, but also for all manner of software deployed.

Software vendors should also embrace the use of standardized software license management tools (see the following section) to simplify the responsibility of cloud subscribers and cloud providers in complying with the licensing agreements.

Standards development organizations should develop and promote interfaces and processes that will enable the implementation of software entitlement management requirements. This encourages the development of common tools used by cloud subscribers, ISVs, and cloud providers. In order to fully realize the value of virtualization and cloud technologies, standards are needed to sufficiently identify licensed software products, and to trace and gather the use of the software and other entitlement usage metrics across the span of deployments.

Solution providers should create and deploy solutions that are open, multi-vendor, and interoperable—working across software provided by different vendors. They should include data models and protocols to allow checking of entitlement prior to activation as well as recording actual use, both for billing and audit purposes.

Consideration should be given to privacy and commercial confidence in these facilities, such that subscribers cannot see the terms and levels of usage of other subscribers. Similarly, ISVs should not be able to view the terms of competitors.

Cloud service providers should clearly communicate how their offerings map against the "ODCA^{SM} Software Entitlement Management Framework."

---

5 See www.opendatacenteralliance.org/index2.php?option=com_productsearch&view=lightbox&proid=14

21

APPENDIX 1: LICENSING MODELS

The use of licensed software products is typically governed by one or more software entitlement models. Commonly used entitlements include:

- **Named user.** The Named User Plus metric is used in environments where users and devices can be easily identified and counted. Named User Plus includes both human and non-human operated devices. Some software vendors expect a minimum number of users per CPU.

- **Client access license (CALs).** A CAL is a license that gives a user the right to access the services of the server. Models include the user-based CAL, device-based CAL, and internal/external-based CAL.

- **Node locked.** The license is locked to specific hardware.

- **Floating/ Concurrent user.** Limits the license to a maximum number of concurrent accesses by discrete, individual users, or devices.

- **Feature.** The license is based on one or more specific "features" within a software product.

- **Site.** Licensing is determined by physical geographical location or logical location within an enterprise entity (for example, a product line).

- **Subscription.** The subscription license applies within a specific timeframe. This can also be a combination of number of users for a specific time frame, as typically offered within SaaS deployment models.

- **Instance.** Licensing is determined by each installation on each given computing device.

- **Capacity.** Licensing is based on one or more of the following capacity attributes associated with the computing platform:

  - **MIPS** – number of CPU cycles.

  - **Processor** – licensed to execute on a maximum number of CPUs. All processors where software is installed and/or running must be licensed. The number of required licenses is determined by multiplying the total number of cores of the processor by a core processor licensing factor, which differs based on vendor and processor models.

  - **Processor value unit (PVU) licensing** for distributed software differentiates licensing of software on distributed processor technologies, as defined by processor vendor, brand, type, and model number.

  - **Virtualization capacity license** – lower of PVUs for the maximum number of virtual cores in the VM available to the eligible product or physical cores in the server available to the eligible product.

  - **Sub-capacity licensing** – licensing of a PVU-based software program for less than the full processor core capacity of the server, when the software program is deployed in an eligible virtualization environment. With full capacity licensing, customers must obtain PVU license entitlements for all activated processor cores in the server, regardless of how the software was deployed.

  - **Cores** – licensed to execute on a maximum number of physical cores.

- **Usage/Transaction based.** Software charged on use and volume, such as the number of clicks, invoices, and transactions.

- **Type of use.** Commercial (business use), personal use, not-for-profit enterprises, educational licenses, and so on.

- **Term of use.** A term license extends for a specific, limited period of time. A perpetual license consists of a one-time license fee that allows continued use of the software program for as long as the customer complies with all terms of the license agreement.

- **Enterprise characteristics**

  - Unrestricted enterprise licenses, used, for example, by a specific line of business or organization structure

  - Licensing driven by the number of employees, financial metrics of the enterprise, or other similar factor

  - SPLAs enable service providers and ISVs with a hosted offering to license products on a monthly basis to provide services and hosted applications to end customers.

- **Constraints and obligations for software licensing.** The software vendor also places certain constraints and obligations on the software user, through dimensions such as

  - Where the software can be installed (what type of hardware device, the hardware make and model, operating system characteristics, geographical location)

  - Duration the software can be used

  - Ability to restrict the transferability of the license

  - Usage restrictions, such as the maximum number of unique users, installs, unique devices, processors, virtual processors, and system memory, and secondary use rights