BSA | The Software Alliance

NAVIGATING THE CLOUD

Why Software Asset Management Is More Important Than Ever

CONTENTS

Executive Summary

The advent of cloud computing was supposed to mark the beginning of the end for license compliance worries. Service providers would simply provision the computing resources needed from remote servers — and be charged accordingly. No hassle. No confusion. No inadvertent piracy. And no legal jeopardy.

An organization must know which software assets it is entitled to, the actual use of those assets, and the impact that moving to the cloud will have on those assets. Adopting cloud architecture without properly addressing SAM-related considerations can result in serious errors associated with cost and risk analysis.

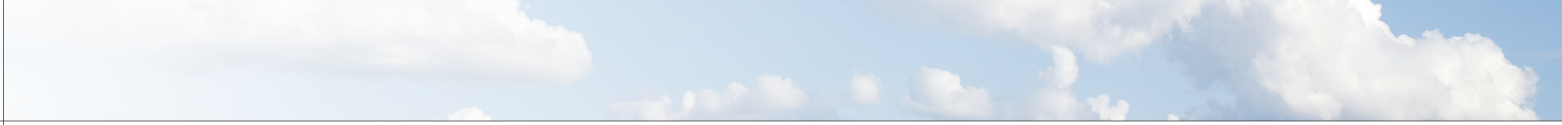
To date, little practical guidance has been available on why and how to deploy SAM in a cloud environment. This whitepaper aims to fill a void and provide guidance on challenges organizations face in successfully integrating and performing SAM within their cloud computing environments.

Cloud computing takes many forms to serve diverse needs in the marketplace. And while it solves some license compliance challenges, it also creates new ones. That is where software asset management comes in.

Software asset management is already being adopted broadly within business environments. Given the benefits of SAM — cost and risk reduction, and increased operational efficiency, to name a few — that is unsurprising. Today, SAM is an integral part of the control framework of any well-run business.

Is SAM still necessary if a company moves to the cloud? The answer is an unequivocal yes. Although cloud services are different than traditionally distributed software in important respects — the need to effectively manage the lifecycle of software assets is equally compelling in a cloud environment.

Both SAM and cloud computing are complex concepts that are still evolving. Given the unique impact that various cloud approaches have on SAM, organizations will find that transitioning to the cloud will likely change the emphasis of their SAM programs. Organizations should carefully and proactively consider the impact their cloud strategy has on their SAM programs in general and specifically on their software licensing.



Cloud Computing

Cloud computing is a model in which computing resources are abstracted from their underlying physical hardware elements. These virtualized services provide scalable, on-demand access to a pool of computing resources typically accessed over the Internet. Many different combinations of virtualized computing resources are offered as cloud computing services but generally can be categorized into one of three primary models: Software as a Service (SaaS), Platform as a Service (PaaS), or Infrastructure as a Service (IaaS). SaaS involves the provision of an on-demand software application delivered via a web client. PaaS provides a computing platform that typically includes an operating system, middleware, and/or a database upon which organizations can build and run software applications. IaaS provides utility computing infrastructure that typically includes a hypervisor, storage, networking and other resources, upon which organizations can build platforms and software applications. Each cloud computing model, when successfully delivered and employed, can provide many benefits to an organization, including scalability, agility and speed-to-market, and cost control.

Software Asset Management

Software Asset Management is the practice of managing the lifecycle of software assets within an organization. One objective of SAM is compliance with the organization's software license agreements. The International Organization for Standardization (ISO) has issued the global standard for SAM (19770-1), which defines the necessary processes and outcomes for achieving effective SAM.

SAM is applicable to and necessary for all organizations using software. SAM, however, becomes an even more critical competency for organizations moving to implement cloud architectures. While effective SAM is a cloud enabler, ineffective SAM can undermine many of the financial advantages and other benefits provided by cloud computing.

SAM in the Cloud

Once an organization moves an operation to the cloud, its SAM program must adapt to address the new and varied challenges presented by cloud architecture. While SAM principles remain unchanged, licensing risks and the application of effective SAM in the cloud differ fundamentally from those in traditional IT environments. SAM programs must be able to completely and accurately measure hardware and software in the new architecture with all its complexities and nuances.

In the cloud, SAM must address the management of assets as well as the management of services. SAM becomes even more real-time given the rapid pace of change in cloud environments where services are provisioned, configured, reconfigured, and released in a matter of minutes. The risk of rogue organizational implementations in the cloud by departments or individuals is ever-present given the ease and speed of provisioning — a process that may bypass the traditional IT, procurement, and SAM gateways. SAM in the cloud needs to address this new risk. Organizations must now consider many new elements in calculating total cost of ownership (TCO), including hidden cloud service costs, additional software licensing costs resulting from deploying software in the cloud, and other costs. Other technology trends such as bring your own device (BYOD) pose unique risks in conjunction with the cloud, which SAM must also address.

SaaS environments pose many licensing challenges for SAM. Organizations may be exposed if the Cloud Service Provider (CSP) infringes on third-party IP rights in providing their solution. Unauthorized use of SaaS accounts poses other compliance risks. These may include accessing the service from prohibited geographies, sharing user accounts, allowing systems to pose as users, or providing access to non-employees (such as contractors, vendors, or customers) where such access is prohibited. Some SaaS solutions include plug-ins or other user-side software that require proper licensing and management. A common misperception holds that shelfware (software paid for but not used) disappears in SaaS situations. A mismanaged SaaS environment with ineffective SAM, however, could lead to a material negative financial impact through overpaying for services not used or needed.

PaaS and IaaS cloud delivery models pose other licensing challenges to SAM. Virtualization, upon which these cloud models are based, may not be permitted in some software license agreements. In other cases, virtualization may carry significant cost implications, such as the need to license all physical processors in the underlying hardware, as opposed to the virtual processors allocated to the specific virtual machine on which the software is installed. The measurement of hardware metrics in a virtualized environment becomes more complex because of the additional degree of separation between software and hardware. An organization may lose access to and the ability to measure such hardware metrics to the software publisher's satisfaction. Furthermore, the transfer of licenses to the cloud may be prohibited, carry restrictions, require pre-approval by the software publisher, or involve additional costs. Additionally, reclaiming an organization's licenses back from the cloud may not be permitted.

If the organization has traditional software license agreements with software publishers for on-premise use, moving these on-premise licenses to now cover use in the cloud does not relieve end-user organizations of their commitments to the software publishers, nor does it relieve them from liability for any non-compliance. Similarly, if a CSP makes software available to an organization in a manner for which the CSP was not properly licensed, the risk of intellectual property infringement may reside with the organization as the beneficiary from such infringement. Depending on contractual terms, the organization may or may not have recourse available against the CSP once a liability has been established. This recourse, however, if it exists, is only after the fact, leaving the organization to shoulder the burden of addressing the liability.

A SAM program should be fully involved in all facets of cloud strategy, design, implementation, operation, and monitoring. While the cloud brings multiple benefits to organizations, SAM can help organizations realize cloud benefits while also mitigating the associated risks.

SAM in the Cloud — Where to Start

SAM programs need to adapt to the cloud. While the nature of the adaptation and the priorities of those efforts will depend on an organization's circumstances, the following are some suggested high-level areas to start with:

- SAM should be fully embedded in the cloud management process, from the initial planning and design of the architecture, to contracting and negotiations, to monitoring the CSP compliance with Service Level Agreements (SLAs), to designing and implementing controls over software assets, and to verifying the CSP billing;
- SAM functions should review their current traditional software license agreements and discuss with their software publishers to understand the rules governing the use of their software in the cloud. If the cloud is part of the organization's strategy and future direction, renegotiation of some software license agreements may be required;
- SAM functions should initiate organization-wide policies governing the cloud to address, among other issues, the process for provisioning and releasing cloud services, required approvals and notifications, required controls, and the required terms and conditions to be included in cloud arrangements; and
- SAM functions should gain visibility to and review all current cloud arrangements that the organization has (IaaS, PaaS, or SaaS), review the actual contracts, and understand what software assets are being used in the cloud and what potential licensing and other SAM related risks may exist.

This paper was written at the request of BSA by principals of Anglepoint Group, Inc. Anglepoint is a global professional services firm providing software asset management, contract compliance and other licensing related services to Fortune 500 clients. The subject matter of this paper is constantly evolving, bringing new threats as well as new solutions, and as such, this paper is not to be considered exhaustive nor does it constitute professional advice.

Key Takeaways

- Cloud computing did not end license compliance worries, but rather created new ones. These challenges could be overcome with effective software asset management;
- Software asset management is as critical for organizations moving to the cloud as it is for organizations running traditional on-premise IT environments. Effective SAM is a cloud enabler;
- While the goal of SAM does not change with the cloud, the "how" of SAM does need to be adapted for cloud environments;
- SAM should be an integral part of an organization's cloud strategy and implementation plan, and be fully embedded in all stages of the cloud management process;
- SAM should further be adapted to manage the cloud service as a whole, beyond the management of just the underlying assets. SAM in the cloud should rely more on policies and automated controls in order to address the dynamic and real-time nature of cloud provisioning;
- Traditional software license agreements require special attention when a move to the cloud is considered to ensure license compliance. It is recommended that the organization works closely with the software publisher on such moves;
- BYOD may represent additional risks to organizations, particularly in conjunction with cloud services; and
- Software as a service introduces potential challenges related to unauthorized use and shelfware.

Introduction to Cloud Technologies

A baseline definition of cloud computing and related concepts is provided below. However, it should be noted that cloud technologies, platforms, and approaches continue to rapidly evolve.

The National Institute of Standards and Technology (NIST) defines cloud computing as[1]:

> a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Cloud computing is gaining momentum due to a convergence of multiple trends including: the maturity of virtualization and virtualization management technologies; Big Data (the collection, storage, management, and analysis of very large data sets); the spread of affordable, high-capacity broadband networks; and the proliferation of mobile connected devices, among others.

Cloud Service Models

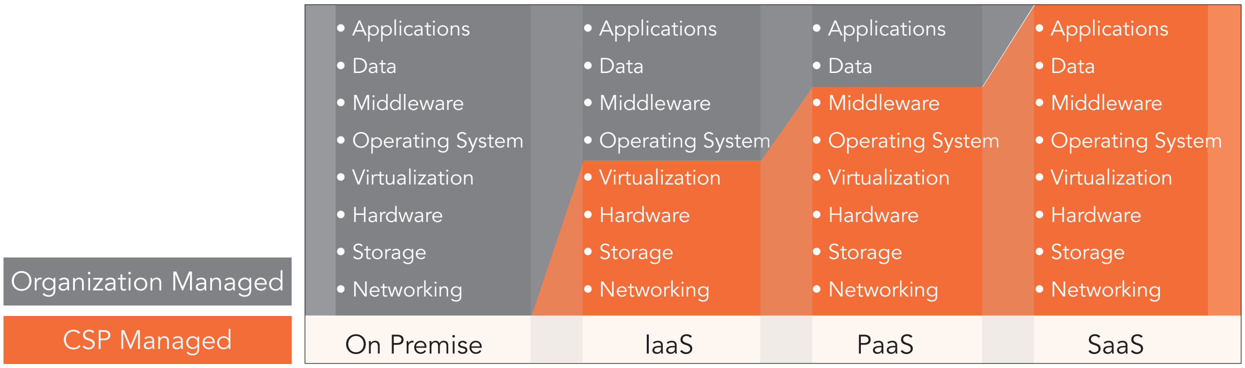
Cloud computing providers use various service models. Actual cloud solutions may involve any combination of approaches. The three most common service models, as defined by NIST, are detailed below.

Software as a Service (SaaS): The capability provided to the customer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., web-based email), or a program interface. The customer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.

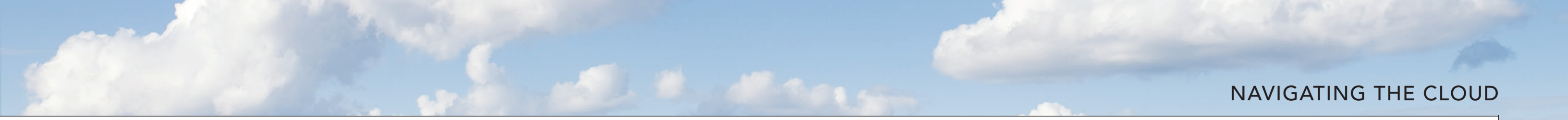
Platform as a Service (PaaS): The capability provided to the customer is to deploy onto the cloud infrastructure customer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The customer still does not manage or control the underlying cloud infrastructure but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

Infrastructure as a Service (IaaS): The capability provided to the customer is to provision processing, storage, networks, and other fundamental computing resources. The customer is able to deploy and run arbitrary software which can include operating systems and applications. The customer again does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (e.g., host firewalls).

Traditional IT architecture may be described as including eight key components. The following chart demonstrates how responsibility is shifted for each component under each of the three cloud service models between the organization and the CSP:



	On Premise	IaaS	PaaS	SaaS
Applications	Organization Managed	Organization Managed	Organization Managed	CSP Managed
Data	Organization Managed	Organization Managed	Organization Managed	CSP Managed
Middleware	Organization Managed	Organization Managed	CSP Managed	CSP Managed
Operating System	Organization Managed	Organization Managed	CSP Managed	CSP Managed
Virtualization	Organization Managed	CSP Managed	CSP Managed	CSP Managed
Hardware	Organization Managed	CSP Managed	CSP Managed	CSP Managed
Storage	Organization Managed	CSP Managed	CSP Managed	CSP Managed
Networking	Organization Managed	CSP Managed	CSP Managed	CSP Managed

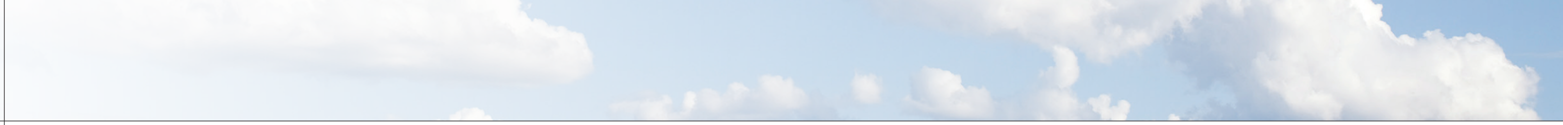


Cloud Deployment Models

Cloud technologies could be offered using various deployment models. The most common deployment models, as defined by NIST, include:

Private cloud:	The cloud infrastructure is provisioned for exclusive use by a single organization (customer) comprising multiple internal customers (e.g., business units). It may be owned, managed, and operated by the customer, a third party, or some combination of them, and it may exist on or off premises.
Community cloud:	The cloud infrastructure is provisioned for exclusive use by a specific community of customers from organizations that have shared concerns (e.g., mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organizations in the community, a third party, or some combination of them, and it may exist on or off-premises.
Public cloud:	The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organization, or some combination of them. It exists on the premises of the cloud provider.
Hybrid cloud:	The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardized or proprietary technology that enables data and application portability (e.g., cloud bursting for load balancing between clouds).

A popular and fast-growing segment of the public cloud, known as the personal cloud, provides services to individual consumers. Personal cloud services include social media, personal email, document creation and editing, music/photo/video/file storage, and many others.



Introduction to Software Asset Management

The Information Technology Infrastructure Library (ITIL) defines Software Asset Management[2] as:

> All the infrastructure and processes necessary for the effective management, control, and protection of the software assets within an organization throughout all the stages of its lifecycle.

The following functional definitions further advance the above standard definition:

> SAM is the practice of effectively managing what an organization does and does not do with software. It is a set of managed processes and functional capabilities to manage the software assets throughout the five stages of their lifecycle (planning, requisition, deployment, maintenance, and retirement).

Software License Management (SLM) is the application of SAM to licensing (measuring and managing license entitlements and license consumptions).

Software License Compliance (SLC) is a subset of SAM and SLM and is the act of ensuring compliance with the terms and conditions governing the licensing and use of software. Software license compliance is a key objective of SAM. In order to ensure compliance with its software license agreements, an organization should perform periodic reconciliation between license consumption and license entitlement. License consumption information is obtained by analyzing complete and accurate software deployment information, including a count of licensing metrics (which vary by product), the application of licensing rules, product use rights, and other information (for example, product bundling rules). License entitlement information is obtained by analyzing complete and accurate purchase histories, software license agreements, and other information such as product name migrations and related licensing rules.

As implied above, SAM has the following characteristics:

- SAM is a business practice, involving people, processes, and technology;
- SAM includes a set of managed processes and functional capabilities. Tools can help facilitate, and in some cases automate, these processes and capabilities; however, deploying a tool by itself does not ensure the effective practice of managing software assets;
- SAM is about all software for which an organization deems it necessary to set governing policies. As such, it is not just about software on desktops. In fact, SAM is most importantly about software on servers given that is where the cost of software assets — as well as their operational impact — is most concentrated. Interestingly, cloud is all about software on servers as well. SAM may also address software on phones, storage arrays, switches, printers, storage media, and other devices; and
- SAM is a multi-disciplinary practice. To be effective, SAM cannot function in a departmental silo, but requires collaboration among several departments, including IT, Finance, Procurement, Legal, HR, and others.

Effective SAM results in the ability to know, with reasonable completeness and accuracy, on a consistent and repeatable basis, the software asset entitlements that are owned, the software assets that are deployed, and where and how the assets are being used. This competency serves multiple objectives, including SLM, SLC, information security, business continuity, change and configuration management, and license compliance.

Effective **information security** requires the identification of all hardware and software assets across the organization, to ensure these assets are authorized to be deployed, are authentic/genuine (i.e.,not tampered with), and are configured with the latest security patches released by the software publisher to protect against security vulnerabilities. Effective **business continuity** requires knowing which assets support which business processes, as well as identifying any interdependencies between assets. It also requires the ability to rebuild any server, down to the required version/patch level of all software components. Effective **change and configuration management** requires knowing that no unauthorized changes are being made to machine configurations which, in turn, requires knowing which machines an organization has, their locations, and their configurations.

SAM Standards

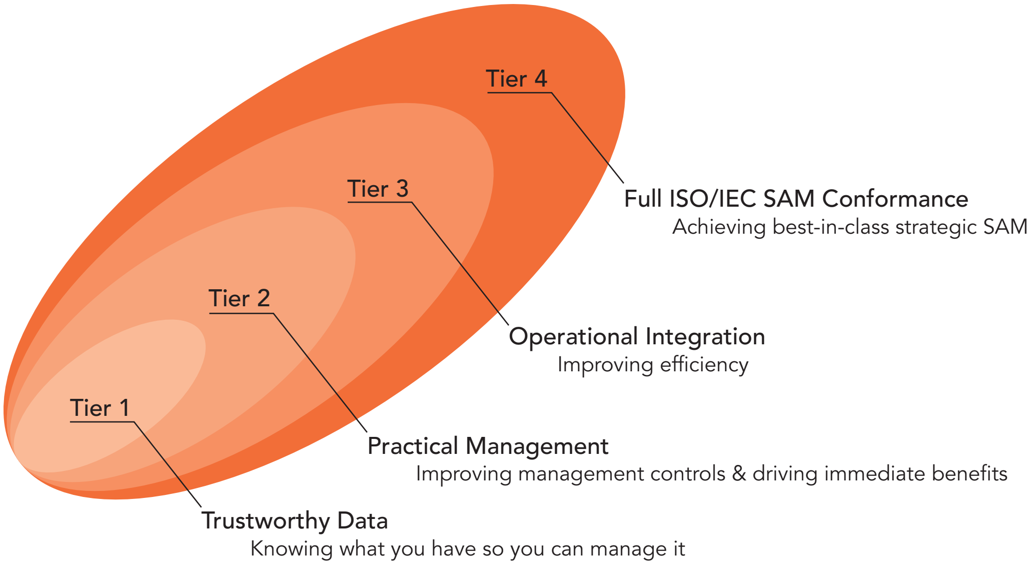
The International Organization for Standardization (ISO) is the largest and most recognized global standards-setting body. ISO's 19770[3] family of SAM standards represent the only global standard for SAM.

19770-1 SAM Processes

Published first in 2006 and revised in 2012, this standard focuses on SAM processes and tiered assessment of conformance. The standard identifies four tiers of SAM adoption, all centered on outcomes.

BSA's SAM Advantage Course[4] is the first industry SAM course aligned to ISO/IEC 19770-1:2012 standard.

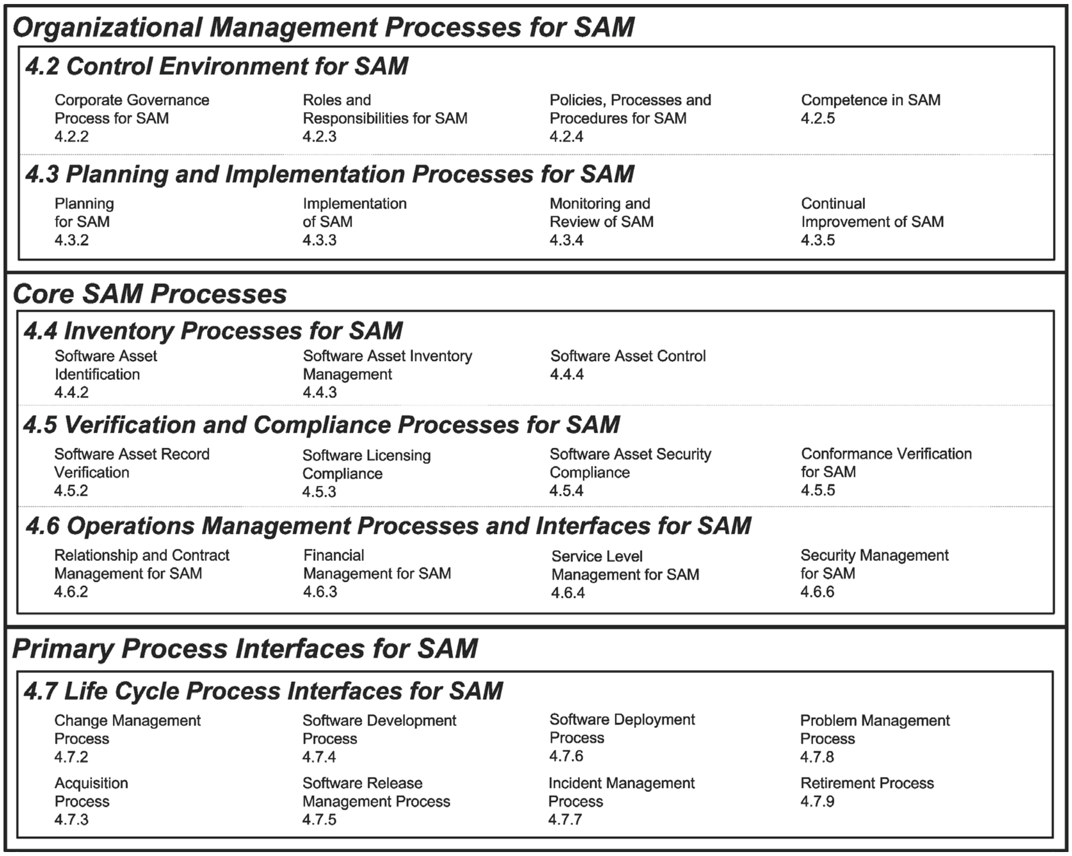
ISO 19770-1 TIERED ASSESSMENT FRAMEWORK


Tier 4
Full ISO/IEC SAM Conformance
Achieving best-in-class strategic SAM
Tier 3
Operational Integration
Improving efficiency
Tier 2
Practical Management
Improving management controls & driving immediate benefits
Tier 1
Trustworthy Data
Knowing what you have so you can manage it

ISO/IEC 19770-1 identifies an integrated set of processes found within SAM as well as a tiered approach to focus their implementation. The 27 identified processes are classified under three major categories and six sub-groups. The four-tiered implementation approach is based on achieving specific results of conformance from the processes.

ISO/IEC 19770-1 applies to all software as well as all technological architectures. It is as relevant to an office productivity application installed on a laptop as it is to an application offered under a SaaS offering in a cloud computing environment.

ISO 19770-1 SAM PROCESSES FRAMEWORK



Organizational Management Processes for SAM

4.2 Control Environment for SAM

Corporate Governance Process for SAM 4.2.2

Roles and Responsibilities for SAM 4.2.3

Policies, Processes and Procedures for SAM 4.2.4

Competence in SAM 4.2.5

4.3 Planning and Implementation Processes for SAM

Planning for SAM 4.3.2

Implementation of SAM 4.3.3

Monitoring and Review of SAM 4.3.4

Continual Improvement of SAM 4.3.5

Core SAM Processes

4.4 Inventory Processes for SAM

Software Asset Identification 4.4.2

Software Asset Inventory Management 4.4.3

Software Asset Control 4.4.4

4.5 Verification and Compliance Processes for SAM

Software Asset Record Verification 4.5.2

Software Licensing Compliance 4.5.3

Software Asset Security Compliance 4.5.4

Conformance Verification for SAM 4.5.5

4.6 Operations Management Processes and Interfaces for SAM

Relationship and Contract Management for SAM 4.6.2

Financial Management for SAM 4.6.3

Service Level Management for SAM 4.6.4

Security Management for SAM 4.6.6

Primary Process Interfaces for SAM

4.7 Life Cycle Process Interfaces for SAM

Change Management Process 4.7.2

Acquisition Process 4.7.3

Software Development Process 4.7.4

Software Release Management Process 4.7.5

Software Deployment Process 4.7.6

Incident Management Process 4.7.7

Problem Management Process 4.7.8

Retirement Process 4.7.9

19770-2 Software ID Tags

ISO/IEC 19770-2 is focused on Software ID Tags (SWID). Published in 2009, its main objective is to establish a framework that provides a complete and accurate identification of installed software, which benefits both software publishers and end-user organizations.

19770-2 defines both mandatory and optional elements within a SWID tag. The SWID tags use standardized XML placed at predetermined locations on machines when the corresponding software is installed.

TagVault[5] (tagvault.org) is a non-profit organization established to facilitate the implementation of 19770-2 by hosting a central tag repository.

Multiple software publishers have embraced the standard and now ship new software with SWID tags. For publishers who are not yet supporting SWID tags, as well as for legacy software products, an organization may use self-created or third-party SWID tags.

The use of SWID tags enables an organization to quickly identify, with increased accuracy, software deployed within its environments. In an IaaS/PaaS environment, the use of self-created SWID tags may enable organizations to differentiate their own software from software provided by the CSP or software of other customers. Therefore, SWID tags, which are increasingly part of SAM in all environments, may become particularly relevant in facilitating the management of software assets in the cloud.

Future ISO SAM Standards: ISO is currently working on a number of future standards, including 19770-3, which will focus on software license entitlement tags, and 19770-7 which will address the management of 19770-2 and 19770-3 tags.

General Considerations for SAM in the Cloud

As it relates to software licensing, each of the different cloud service models carries specific risks and requires specific considerations which are discussed over the next few sections. This section covers, at a high level, some of the general considerations for SAM across all cloud service and deployment models.

Adapting SAM to the Cloud

Cloud computing does not preclude an organization's need for SAM. The cloud environment is simply a different infrastructure where SAM processes need to operate effectively. Organizations must tailor their implementations of the 27 process areas in ISO 19770-1 to take into account the nuances of the software and architectures within their cloud environment. Just as organizations must adapt their approach to handle the differences between physical and virtual environments, they must adapt their approach to handle the cloud environment.

Organizations need to specifically address cloud computing within their policies and procedures to fulfill their ISO 19770-1 requirements. Key considerations to address when implementing SAM in the cloud include:

- *Changing nature of software assets.* Traditional (pre-cloud) SAM focuses solely on managing the lifecycle of the underlying software assets. With the cloud, SAM programs are now required to manage the cloud service, whether in place of or in addition to managing the software assets. In a way, the cloud service itself becomes an asset that requires managing. Given that certain aspects of SAM are now delivered via the CSP and not owned by the customer, SAM programs need to monitor a CSP's compliance with its service level agreements (SLAs) and other applicable requirements. The ability to perform such monitoring effectively represents a new mindset, a new skill set, and a new toolset that SAM programs need to develop.

- *Real-time SAM.* One of the business benefits of the cloud is its agility and speed-to-market. Cloud services can be provisioned or released with a few mouse clicks. Many traditional (pre-cloud) SAM processes assume longer lifecycles, allowing more time for planning, contracting, periodic discovery and reconciliations, and other SAM control activities. With the cloud, SAM programs must adapt to a more real-time environment by designing processes to allow for faster reaction and relying more heavily on detailed policies and processes on cloud contracting, deployment, and management across the organization.

- *Decentralization.* Cloud services, particularly SaaS, are generally easy to implement and may not require significant IT knowledge or resources. As such, many organizations find that their employees are bypassing normal IT procurement processes to deploy cloud services. SaaS providers may target the business buyers directly (e.g., sales or HR departments) rather than going through the traditional IT buyers. Cloud services are typically considered operational expenses, bypassing the more rigorous approval processes that may be in place for capital expenditures. In fact, cloud services can often be paid for using a corporate credit card, bypassing normal procurement/finance approval gateways. Because of these factors, IT and SAM functions may learn about some cloud implementations only after the fact (or not at all) and, therefore, would not be involved in the contracting phase. This may result in a number of challenges:

  - *Weak contracting.* The SAM function, IT, and procurement may not be sufficiently involved in the contracting phase;

  - *Increased license compliance exposure.* The SAM function may not be involved in designing, contracting, and monitoring the cloud solution with respect to licensing risk;

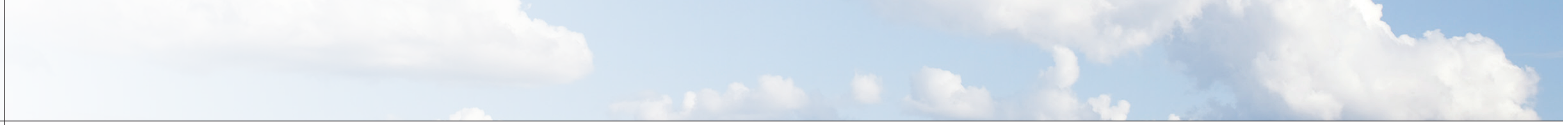
  - *Loss of control over where an organization keeps its data.* The loss of control may result in privacy, information security, and business continuity exposures;

  - *Loss of control over an organization's operational dependencies.* Challenges may be acute, particularly when the organization becomes dependent on a rogue cloud solution to run its business;

  - *Lack of known limits to cloud spend/no final cost.* In some cases, user actions may commit the organization financially with respect to cloud services. For example, users may activate or use additional functionality or they may exceed their baseline-provided data storage limit. This is in addition to the lack of IT control over the department or user initiating the cloud service as a rogue initiative in the first place; and

  - *Loss of financial visibility.* Given that departments or individual employees can procure cloud services directly, some costs may be classified incorrectly, and organizations may lose financial visibility to their overall IT and cloud spend.

- *Understanding total cost of ownership (TCO) in the cloud.* Part of any SAM program is the understanding of total costs and budgets associated with managing software assets across all stages of their lifecycle. SAM programs should be able to understand and budget for costs associated with traditional software license agreements. The cloud is a different environment with different types of contracts, requiring the development of new skills sets and capabilities for SAM programs. While cloud agreements may seem straight-forward, they can include multiple direct, indirect, and hidden costs that need to be accounted for and understood. Some of these costs may include the cost of migration to the cloud, integration with other IT systems, oversubscription to cloud services, need for premium support services, additional storage requirements, costs for data extraction, costs of changing the scope of the services, and rising service renewal costs. Additional costs may result from the highly virtualized nature of the cloud which is not always supported under traditional license grants.



Bring Your Own Device

One of the main benefits of cloud models is Internet accessibility. This characteristic of the cloud is converging with BYOD, another IT trend. BYOD is about organizations permitting employees to access corporate information and applications using personally owned devices (laptops, tablets, smartphones). Cloud is a good fit with BYOD because it is typically accessible from anywhere. Many SaaS providers offer specifically designed apps for BYOD-type devices, allowing the user to take full advantage of the service. From a SAM standpoint, BYOD presents additional risks as it relates to the cloud:

- *License to access from mobile devices.* Organizations need to be properly licensed to access their cloud software from all devices. Depending on the terms and conditions of the software license agreements, BYOD access may be prohibited or carry additional license fees.

- *Security concerns.* Given that the organization does not control the security configurations of BYOD or of the connection between BYOD and the cloud (which may be over personal cellular/Wi-Fi), additional information security risks may result.

- *Personal cloud and use of personal apps for business use via BYOD.* The nature of BYOD is such that it allows easy access to personal apps that are based on personal cloud services (for example, productivity apps such as note-taking or managing to-do lists). Given that those personal apps are available to the user on the same devices used to access corporate apps and data, it is highly likely that users will use such personal apps for business purposes as well. However, the license terms on such personal apps may prohibit their use for business/commercial purposes, exposing both the employee and the organization to additional licensing risks. In addition, corporate information may thus reside on personal clouds over which the organization has no knowledge or control, leading to additional information security and privacy risks.

- *Counterfeit and pirated software risks with BYOD.* Organizations have little control over what software employees are downloading and installing on their personal devices, where such software is coming from, and whether the employee is properly licensed to install and use it. This presents multiple risks to organizations given that such unknown software may not be genuine and may thus pose a risk to the entire device and the corporate data accessed through it (even if the software itself is not used to access any corporate data, risk may still result by the software being installed or running on the same device). Also, if the employee actually uses such pirated software for business purposes (as described above) this may expose the organization to license compliance and information security risks.

Facilitating Regulatory and Data Security Compliance

Many organizations have regulatory or other business requirements to consider related to their data privacy and information security. Ensuring data is protected is a common priority of all organizations, but some organizations have regulatory or other business requirements to not only protect their data, but to provide certifications or other assurances that the data is in fact protected.

One such business compliance requirement is PCI DSS. PCI DSS is a proprietary information security standard for organizations that handle cardholder information for major credit, debt, prepaid, ATM, and other cards. In order to achieve and maintain a PCI DSS certification, organizations are required to perform annual validations. To complete the annual validation, the organization must know their infrastructure (hardware, software, networking, firewalls, etc.) details. Organizations that process large volumes of data require onsite visits to validate compliance. Implementing cloud environments may significantly challenge the ability to maintain regulatory compliance if not adequately planned.

The following sample laws and regulations provide numerous other regulatory requirements for organizations to follow related to data location, access, security, etc.:

- US-related:
  - Sarbanes-Oxley (SOX);
  - Health Insurance Portability and Accountability Act (HIPAA);
  - Electronic Records and Electronic Submissions CFR 21 part 11;
  - Financial Modernization Act of 1999;
  - Federal Desktop Core Configuration (FDCC); and
  - USA PATRIOT Act and US Presidential Executive Order 13103.
- Non-US-related:
  - European Union — Data Protection Directive, and other specific legislation in EU member states;
  - Australia — Corporate Law Economic Reform Program Act 2004 (CLERP9);
  - Malaysia — Personal Data Protection Act 2010;
  - India — The Institutes of Technology (Amendment) Act, and Clause 49 of the Listing Agreement to the Indian Stock Exchange; and
  - South Africa — The King Report on Corporate Governance.

Data privacy is a key area of concern with the cloud. Specifically, the European Union's Data Protection Directive generally prohibits the transfer of personal data to non-European Union countries that do not meet the European Union (EU) "adequacy" standard for privacy protection. As the United States takes a different approach to privacy, a mechanism was put in place to bridge these differences and provide a streamlined means for organizations operating in the US to comply with the EU directive. Therefore, the US Department of Commerce, in consultation with the European Commission developed the "Safe Harbor" framework. Organizations can join the Safe Harbor program if they meet its criteria which is based on a set of privacy principles. These principles include notice related to the collection of personal data, choice as to how this data may be used, and security and precautions to protect the collected data. Note, though, that Safe Harbor is just one option to ensure lawful transfer of data. Therefore, organizations may need to consider other options to ensure that their governance of private information and data is lawful in the cloud.

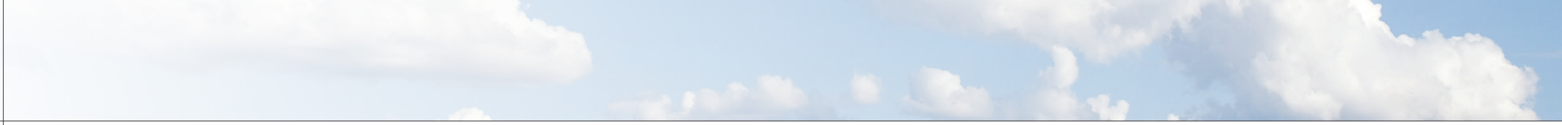
The impact of these complexities introduced by cloud architecture fundamentally affects how organizations need to manage their SAM programs. Regardless of the type of cloud service, SAM programs now must align themselves with the organizational group (or groups) responsible for managing regulatory and data security compliance almost as an extension of their own team. Ignoring SAM or diminishing its authority relative to the cloud may result in additional risks and costs and may negate other benefits gained by moving to the cloud.

SAM as a Cloud Enabler

An often-overlooked advantage of an effective SAM program is its ability to help form the organization's strategies for the future. Detailed knowledge of an organization's hardware, software, and infrastructure can provide a powerful foundation for making well-informed, critical decisions related to growth, acquisition, and other important strategic decisions.

Cloud computing is one such strategy where SAM can provide vital insights. Understanding an organization's current environment (hardware and software) is critical in determining whether or not cloud computing makes business sense.

Organizations cannot optimize what they don't know. Whether the objective is to virtualize on-premise, move to a private cloud, or move to the public cloud (IaaS, PaaS, or SaaS), the organization needs to know which hardware and software assets it has, their locations, their configurations, their users, how they are being used, how they are licensed (including whether such licenses support a cost-effective migration to a cloud environment), and the total costs associated with such assets. Only with complete and accurate asset information can the organization understand the true return on investment needed to make virtualization or cloud computing a benefit. SAM is therefore a core competency for enabling a move to the cloud.



SAM Considerations for Software as a Service

Software as a Service is a subscription service most commonly accessed via a web browser. Leading examples of SaaS include Salesforce.com, Microsoft Office 365, Google Apps, and NetSuite, among others.

SaaS is typically offered using one of four business models, or some combination thereof:

- *Period subscription.* This is the most common model. Users pay a per-user fee that allows access to the system for a set period of time, usually a year. The fee may vary based on specific services or modules that the user can access.

- *Actual usage.* Currently a rare model where fees are calculated based on measures such as the number of logins to the system, the duration of use, the amount of data stored, the number of transactions, or any variations of the above.

- *Business results.* Currently a rare model where the SaaS provider charges based on actual results obtained from using the service (for example, a certain percentage of the revenue from each transaction processed), or the customer's business results in general (for example, revenue).

- *Ad-supported.* In this model, customers do not pay a fee. Rather, the CSP is basing the service on revenue from ads displayed to the users. This offering is more common in the personal cloud.

A common misperception is that SaaS is free from licensing risks and may therefore be excluded from the scope of SAM. Licensing risks associated with SaaS vary depending on the SaaS CSP and contract specifics. The following are some of the more common risks:

- *IP infringement:* The SaaS provider may be infringing on intellectual property of a third party, whether knowingly or not. Unless the CSP is contractually required to defend, hold harmless, and indemnify its customers against any and all such IP infringements, the customer may be exposed to legal risks as the ultimate beneficiary of such infringement. As CSPs may operate in a different country than its customers, the CSP may be subject to weaker laws around IP infringement. Furthermore, such infringement, if it exists, may represent a risk to the CSP's ability to provide the service at the current functionality or price point. This may represent further operational risks to the customer who may have become dependent on the service.

- *Client-side software components:* Contrary to the common perception, some SaaS solutions may require the installation of code on the client side. This may be in the form of a browser plug-in, applet, agent, client software, or even a full-blown software suite (such as MS Office Professional suite in the case of a Microsoft Office 365 subscription). The customer needs to: (a) be properly licensed to use such client-side software and have sufficient proof of license in case of an audit or license review; and (b) manage these software assets just like any other software asset to ensure they are accounted for, are not over-deployed, and are used in accordance with the applicable product use rights and restrictions.

  Example: An organization was including a client-side software component of SaaS service as part of its standard PC image. The organization was significantly over-deployed and in breach relative to the number of authorized users and the terms of its SaaS agreement.

- *Unauthorized use:* SaaS typically comes with multiple restrictions on use. In many cases, the restrictions are not negotiable given the nature of SaaS contracts. The customer needs to have proper controls in place to ensure compliance with all contractual requirements and limitations. Such requirements may include, but are not limited to:

  - Limitation on geography. For example, the agreement may allow only US-based employees to access the service (where the SaaS provider charges a different price for non-US users or for other reasons).

  - Restriction on sharing user accounts among multiple employees.

    Example: A department manager provides his individual user access login information for a software training site to his team of 10 people so they all can get the training.

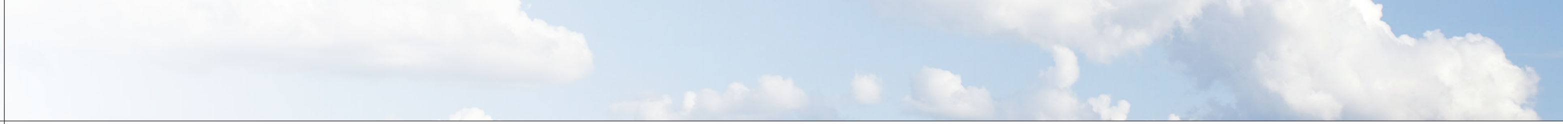
  - Restriction on having a system account access the service (where the “user” is another system and not an individual end-user).

  - Restriction on providing user access to non-employees of customers (for example, contractors, outsource providers, vendors, business partners, customers) or affiliated entities of the customer. Such restrictions, if they exist, can prevent the customer from using the SaaS solution altogether.

  - Restriction on providing reports or information generated from the SaaS system to unlicensed individuals not paying the subscription fee. For example, having a single user account and then e-mailing a report from the SaaS system to an entire team.

Some SaaS providers are implementing analytics to detect unauthorized use. Such analytics may include a review of the following:

- Simultaneous connections of the same user account;
- IP addresses the connection is coming from, which indicate country of origin;
- Time of day the user account is accessed;
- Volume of transactions/data for the user account;
- Comparison of customer profile to publicly available information (for example, the total number of employees at the customer); and
- Comparison of a customer profile to other customers in the same industry, to detect abnormal use patterns.



- *Shelfware:* Contrary to common misperception, shelfware (paying for software not in use) is possible and even likely with SaaS. This is primarily because almost all current SaaS models are not pay-per-use, but rather require an up-front commitment to a certain subscription period (for example, a certain number of users for a 12-month period). The cost of most SaaS arrangements is thus typically not directly aligned to actual usage. End-user organizations may find that they have committed to a level of payment exceeding their needs. This can often occur when entering a new SaaS arrangement (payment starts immediately, however, it may take months for users to get transitioned to the service) or when only a few of the users actually make use of their paid subscription, or as a result of material reduction in size and composition of the customer's workforce while payment to the SaaS provider needs to continue at originally committed levels.

- *Economies of scale:* Some traditional enterprise software licensing models, such as those based on hardware metrics, have a notion of economies of scale, where the end-user is able to increase the demands on the software without necessarily increasing software costs. As organizations transition software models to a user-based SaaS model, they may be abandoning this benefit. This may limit the organization's ability to leverage multiple computing technologies to affect its software costs. For example, no longer is the organization able to address increased demand on the software by upgrading hardware (processor speed, memory, network speed) in a manner friendly to the software licensing model. Instead, each added user of the software results in a direct increase to the cost for a certain fixed contractual period, which may or may not correlate with the period of use actually needed by the organization.

- *SaaS subcontracting:* An additional layer of complexity in SaaS engagements is that many SaaS providers use other providers (e.g., IaaS/PaaS) in the provisioning of their services. For example, a web SaaS service may run its infrastructure via Amazon's cloud-based infrastructure. Some of the issues discussed above are related to and depend upon these additional providers. The organization needs to understand what assurance it receives vis-à-vis the entire SaaS ecosystem.

SAM and Virtualization/ Private Cloud

All non-SaaS cloud technologies and deployment methods are primarily based on — and enabled by — virtualization technology.

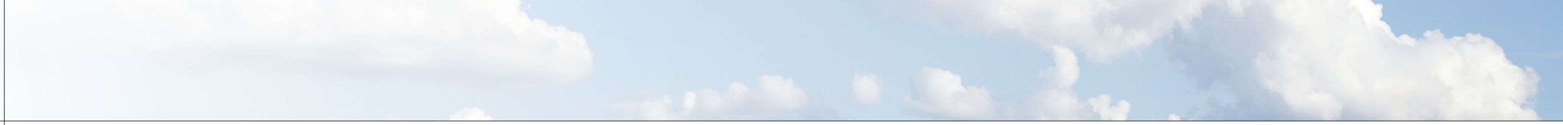
Virtualization involves the deployment of a virtual (rather than physical) version of an IT resource, such as hardware or storage. As a technology, virtualization has been around for decades, starting with mainframe computers. In recent years, virtualization has completely penetrated IT. A full discussion of virtualization technologies is beyond the scope of this paper, but understanding the basic concepts of virtualization is necessary to understanding the challenges of managing SAM in the cloud.

Virtualization involves degrees of separation between software and hardware. Traditional non-virtualized IT involved a one-to-one relationship between hardware and software. One operating system (OS) — or one instance of the software product — tied to one piece of hardware. The most common licensing metrics in the software industry today are still those related to hardware measurement (for example, licensing by processor/core) because hardware was historically the easiest element to measure objectively.

Conversely, virtualization implies a one-to-many relationship between hardware and software. Multiple virtualized machines, each with its own operating system and applications, can now be configured on a single piece of hardware. The hardware resources (for example, CPU or memory) are allocated, often dynamically, between the various operating systems so that peak usage can be addressed by virtual machines.

Virtualization presents a real challenge to hardware metrics-based software licensing, particularly given that many license agreements in effect today did not contemplate virtualization when they were written. Different software publishers have adopted different policies related to measuring hardware metrics in virtualized environments. Many insist the customer be licensed for the maximum potential hardware configuration (for example, all CPUs on the actual underlying hardware) given the dynamic nature of resource allocation in virtualized environments. Some software publishers have different policies depending on whether the virtualization technology being used (or the cloud service being used) is theirs or a third-party's, or whether approved tracking tools are implemented. Customers should review their software license agreements and check with their software publishers to understand the specific rules that apply to them.

New developments in virtualization management technologies that allow a many-to-many relationship between hardware and software may further complicate SAM challenges. Under one scenario, a virtualization layer will buffer between multiple pieces of hardware on one end, and multiple virtual machines (operating systems) on the other end, making it impossible to tie a specific virtual machine to a specific hardware.



Virtualization can bring many benefits to customers, including lowering IT costs, lowering their carbon footprint (power consumption), improving business continuity, and boosting agility and speed-to-market. The licensing implications alone, however, if not properly considered and planned for, may make virtualization impractical from a cost standpoint.

Virtualization presents unique challenges to SAM primarily because of discovery and management. Virtual machines can be created or deleted with a few mouse clicks, and their configurations change frequently and automatically. It is not uncommon for virtual machines to be created in support of ad-hoc needs (such as workload spikes of business units, or test and development needs of R&D groups) and then deleted afterward without involving the SAM function or obtaining the necessary additional licenses for the software used. This dynamic nature of virtualization, coupled with the uncertainty and challenges related to licensing rules (particularly for historical license agreements) makes virtualization one of the biggest challenges to effective SAM today.

Given the licensing challenges associated with virtualization, and in light of its growing presence, software publishers may be taking one of two paths. One approach is to rely less on hardware-based licensing metrics and promote instead more user-based metrics, throughput-based metrics (for example, number of transactions), or results-based metrics (for example, revenue). Another approach is to provide customers with specific tools to collect hardware metrics in virtualized environments (for example, the IBM License Metrics Tool, ILMT). The above approaches may help organizations implement SAM in virtualized environments more effectively with respect to those software publishers. Organizations, however, cannot solely rely on software publishers to solve all, or even most, of the SAM challenges associated with virtualization.

To an end-user organization, the impact of virtualization on SAM is significant. SAM programs must address all virtualized assets in its scope and have comprehensive data over their software licenses that are affected by virtualization. SAM programs need to regularly refresh their understanding of licensing rules as software publishers continue to update their policies. All virtualization-affected software assets must be managed in a deliberate manner so that virtualization deployments do not cause potentially negative financial implications. Additionally, SAM programs will need to regularly review the IT infrastructure for any rogue use of virtualization technology that might be outside the scope of existing management programs.

Another unique SAM challenge of virtualization has to do with de-provisioning discipline. Virtual machines can be created quickly and easily to serve ad-hoc needs. Once the business need is over, however, someone needs to proactively delete the virtual machine, or else the organization will continue to consume additional licenses for no need. Many organizations have a large number of “orphaned” virtual machines which nobody knows what they were created for. SAM programs should implement controls around timely de-provisioning of virtual machines no longer in need.

Software publishers have been developing official guidance and policies regarding the impact of virtualization at varying levels of sophistication. SAM programs can no longer “assume” the impact of virtualization to software licensing even when left “silent” in the software license agreement. Although organizations may not always get the answer they want to hear, having complete clarity on how publishers account for virtualization with regard to licensing is a must for any successful SAM program.

Further complicating SAM is the mixed-metric reality found in virtualized environments. Organizations have likely purchased their software both pre- and post-virtualization, which means they now have different license types of the same software that might be affected differently by virtualization. Organizations must work with software publishers to deploy licenses inside of virtualized environments in a way that is clearly in line with the publisher’s policies or risk unplanned audit related costs.

SAM and Infrastructure/ Platform as a Service

In non-SaaS cloud deployment models (i.e., IaaS/PaaS), some software is provided by the CSP while other software is provided by the organization. Examples of IaaS/PaaS include Amazon EC2, Microsoft Azure, and IBM SmartCloud.

For ***software provided by the CSP*** (for example, the operating system or middleware software), as is the case with SaaS, the customer should obtain assurances that the CSP is properly licensed to provide the software and that the proposed use is covered by the license owned by the CSP. If the CSP makes any non-home-grown software available to its customers, as is likely to be the case, the CSP requires a license from the software publisher that is usually in the form of a service provider license agreement, or equivalent, that allows the CSP to use the software to provide a service to third parties. Customers may want to receive assurances from their CSP that it has the legal right to provide the service. In addition, customers should ask for an indemnity provision in the cloud agreement protecting them from any third party claims that the service infringes IP rights.

Another risk involving software provided by the CSP is the risk of the CSP not using genuine software. If the CSP is using counterfeit software, there is the risk that unauthorized changes may have been made to the code (for example, the inclusion of a Trojan horse virus) that would pose information security risks to the organization. Given that the organization does not have any control over software provided by the CSP, it must ensure in other ways that the CSP only uses genuine software, such as by including contractual terms and working only with reputable/certified CSPs.

For ***software provided by the customer***, it should be noted that the customer is faced with managing and navigating between two separate and distinct contractual arrangements: one with the software publisher and one with the CSP.

The typical inherent disconnect between the organization's relationship with the software publisher and its relationship with the CSP may cause the following challenges and considerations in achieving effective SAM in the cloud:

➲ *Transferring licenses to the cloud.* Pursuant to the license terms, a transfer of a software license to the cloud may require the affirmative consent of the software

The following provision from a license agreement can serve as an example for a limitation on making internal-use software available to third parties (a limitation which a CSP may have if not properly licensed): "Licensee will not lease, lend or rent the Software, use the Software to provide service bureau, time sharing, rental, application services provider, hosting or other computer services to third parties, or otherwise make the functionality of the Software available to third parties."

> In some cases, the CSP is also the software publisher, providing the same software in two delivery forms: traditional/on-premise and in the cloud.

publisher (for example, some software license agreements prohibit by default any off-premise use or deployment on hardware not owned by the organization). Some major publishers have policies that prohibit using their licenses in the cloud, while other publishers create their own clouds, create mechanisms to measure software use in the cloud, and certify some CSPs (but not others) as safe places to use their software. Many other software publishers, however, do not have clear policies. An unpermitted transfer of software licenses to the cloud may expose the organization, and possibly the CSP, to potential liability risk.

- *Unauthorized use.* The license grant may stipulate any number of limitations that may impact the ability to transfer licenses to the cloud. Examples of such limitations include:
  - Limitation on geography — may be particularly challenging to manage given that with some cloud services the customer does not know the physical location (or even country) of the servers;
  - Limitation on legal entities covered by the license grant — may preclude the use of the cloud depending on the specific terms; and
  - Limitation on devices or platform — may preclude the use of certain cloud environments and may be particularly challenging to manage given that in some cloud environments the customer does not know the technical details of the cloud architecture.

- *Measuring hardware-related licensing metrics in the cloud.* Measuring hardware-related licensing metrics in a complete, accurate, and repeatable way is a significant SAM challenge, even under traditional circumstances where the hardware in question is sitting in the customer's own data center. Add the complexities of IaaS/PaaS and the task becomes more challenging. It may be difficult to distinguish software owned/provided by the CSP from that owned/provided by the customer and correctly account for each, risking either over-payment or under-payment of license fees.

- *Software vendor audits.* Most software license agreements include an audit provision, allowing the software publisher, upon notice, to access the customer's environment for the purpose of ascertaining compliance with the terms and conditions of the license agreement. It is highly unlikely that the customer would be able to agree with its CSP on allowing such onsite access to the software publisher, even assuming there was a way for the customer to find out where in the cloud its servers are physically located. The customer may, therefore, be in potential violation of its software license agreement with the software vendor. In some cases, the customer may be able to provide remote access to the auditors into their virtual machines on the cloud. Such access, however, may not be sufficient for software publishers who require licensing for the full metrics of the underlying hardware. Given that the customer is likely sharing such underlying hardware with other customers of the CSP in multi-tenancy, the customer is unlikely to receive access to the underlying hardware from the CSP. In addition, if the license agreement requires the organization to provide certain data within a specified amount of time, the SAM program must work with the CSP to ensure compliance with such requirements can be achieved.

- *Reclaiming licenses from the cloud.* The customer should determine whether, based on its cloud service agreement, software license agreements, and software publisher policies, it could reclaim its licenses upon termination of the cloud engagement. In some cases, the transfer back of licenses may require the consent of the software publisher and/or the CSP.

About BSA | The Software Alliance

BSA | The Software Alliance is the leading advocate for the global software industry before governments and in the international marketplace. It is an association of world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life.

BSA serves as the world's premier anti-piracy organization and as a respected leader in shaping public policies that promote technology innovation and drive economic growth.

Through government relations, intellectual property enforcement and educational activities in dozens of countries around the world, BSA protects intellectual property and fosters innovation; works to open markets and ensure fair competition; and builds trust and confidence in information technology for consumers, businesses and governments alike.

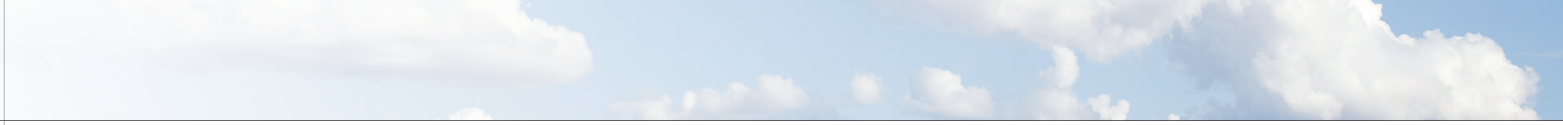
BSA serves as the world's premier anti-piracy organization and as a respected leader in shaping public policies that promote technology innovation and drive economic growth.

Protecting Intellectual Property & Fostering Innovation

Intellectual property rights — copyrights, patents and trademarks — provide the legal framework for creative enterprise, the bedrock of growing economies. They are also essential to commercial software development, which is the world's largest copyright industry.

By working with policymakers, leading enforcement actions and conducting public-education initiatives around the world, BSA ensures that respect for IPR pervades the global economy and society.

- **Championing Intellectual Property Rights:** BSA works with governments around the world to ensure intellectual property protections keep pace with new innovations in technology, such as cloud computing.
- **Curbing Software Theft:** BSA conducts vigorous enforcement programs around the world, helping its members guard against software theft by taking legal action against commercial, end-user license infringement, counterfeiting operations and Internet piracy.



- **Leading Industry Research:** BSA publishes the most authoritative global studies on piracy and its economic impact, illuminating the scope of the problem and helping shape national and international policy responses.
- **Educating the Public:** BSA educates consumers about harms associated with software piracy and offers groundbreaking tools and training programs to help organizations more effectively manage their software assets.

Opening Markets & Ensuring Fair Competition

- Open markets are essential to economic growth and prosperity. BSA expands market opportunities for the software industry by working with governments to break down trade barriers and eliminate discriminatory procurement preferences that stifle innovation by skewing competition.
- **Breaking Down Barriers to Growth:** BSA provides policymakers with information, expert analysis and industry insights to promote an open-markets agenda. These efforts include a special focus on the BRIC economies, which are the world's fastest-growing technology markets but also home to rampant piracy.
- **Promoting Technology Neutrality:** BSA encourages fair competition among technologies by promoting internationally recognized standards and unbiased IT-procurement policies for governments.
- **Supporting New Innovations:** BSA works with policymakers around the world to create conditions for new technologies, such as cloud computing, to flourish. In addition to collaborating on technology standards, this work involves elevating intellectual property protections, harmonizing international legal principles and addressing other challenges that are beyond the capability or jurisdiction of any one company or government.

Building Trust & Confidence in Technology

Security and privacy undergird trust and confidence in information technology for consumers, businesses and governments. BSA promotes responsible data stewardship and facilitates acceptance and adoption of each new wave of innovation that transforms the technology marketplace and creates value for society.

- **Driving Public-Private Collaboration:** Drawing on the expertise of its members and productive working relationships with public officials, BSA serves as a knowledge center and catalyst to encourage cooperation and forge consensus among industry and governments.
- **Protecting Consumers:** As new technologies emerge, such as cloud computing, BSA and its members develop appropriate privacy and security standards and share their insights with policymakers and regulators.
- **Mapping Policy Solutions:** BSA has developed a global cybersecurity framework to guide governments in crafting policies that effectively deter and punish cybercrime, mitigate threats, inform and protect consumers, and respond to cyber incidents.

ENDNOTES

[1] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[2] ITIL V3 Guide to Software Asset Management

[3] http://www.19770.org

[4] https://samadvantage.bsa.org

[5] http://www.tagvault.org

The Software Alliance

BSA

www.bsa.org

BSA Worldwide Headquarters

20 F Street, NW
Suite 800
Washington, DC 20001

T: +1.202.872.5500
F: +1.202.872.5501

BSA Asia-Pacific

300 Beach Road
#25-08 The Concourse
Singapore 199555

T: +65.6292.2072
F: +65.6292.6369

BSA Europe, Middle East & Africa

2 Queen Anne's Gate Buildings
Dartmouth Street
London, SW1H 9BP
United Kingdom

T: +44.207.340.6080
F: +44.207.340.6090

Argentina Australia Belgium Brazil Canada Chile China Colombia Czech Republic Denmark France
Germany Greece India Indonesia Israel Italy Japan Malaysia Mexico Netherlands Panama Peru
Poland Russia South Africa South Korea Spain Taiwan Thailand Turkey Vietnam