
The Software Alliance
BSA
NAVIGIEREN IN DER CLOUD
Ein Leitfaden für effektives Software Asset Management

# Inhalt

# Executive Summary

## Cloud Computing hätte der Anfang vom Ende aller Lizenzschwierigkeiten sein sollen: bedarfsgerechter Remote-Zugriff auf Ressourcen, eine entsprechende Rechnung, fertig. Keine Verwirrung, keine Piraterie, keine rechtlichen Probleme.

Bis heute gibt es kaum praktische Richtlinien für Software Asset Management (SAM) in der Cloud. Dieses Whitepaper soll die Lücke schließen und Organisationen Hilfestellung bei der Integration von SAM-Abläufen in ihre Cloud-Prozesse geben.

Cloud Computing hat viele verschiedene Formen, um den unterschiedlichen Marktanforderungen gerecht zu werden. Und tatsächlich löst es bereits so manches alte Lizenzproblem – allerdings kommen auch neue hinzu. Intelligentes SAM setzt hier an. Entsprechende Konzepte werden bereits in vielen Unternehmen umgesetzt. Angesichts der enormen Vorteile – Kosten- und Risikominderung, die Steigerung der betrieblichen Effizienz und viele mehr – überrascht das nicht. SAM ist heute integraler Bestandteil jedes vernünftigen Betriebsmanagements.

Doch was ändert sich durch den Wechsel in die Cloud? Ist Lizenzmanagement überhaupt noch nötig? Die Antwort ist ein klares Ja. Denn obwohl sich Cloud-Software in vielen Punkten deutlich vom traditionellen Vertrieb unterscheidet, ist die Notwendigkeit eines effizienten Lebenszyklusmanagements in der Cloud eine ebenso große Herausforderung.

Sowohl SAM als auch Cloud Computing entwickeln sich stetig fort und beeinflussen sich gegenseitig. Bereits jetzt ist im SAM eine deutliche Akzentverschiebung spürbar. Organisationen müssen sorgfältig und proaktiv die Auswirkungen ihrer Cloud-Strategien auf ihre Lizenzprogramme bedenken.

Jede Organisation muss wissen, welche Software sie besitzt, wie, wo und wann sie eingesetzt wird, und welche Auswirkungen der Schritt in die Cloud haben wird. Es kann kostspielige und riskante Konsequenzen haben, wenn man handelt ohne vorher die Lizenzfragen sorgfältig zu bedenken.

## Cloud Computing

Cloud Computing bedeutet, dass Computerressourcen von ihren physischen Hardware-Elementen getrennt werden. Diese virtualisierten Dienste ermöglichen den skalierbaren On-Demand-Zugriff auf eine Vielzahl von Ressourcen, typischerweise über das Internet. Trotz der nahezu unendlichen Kombinationsmöglichkeiten haben sich drei grobe Kategorisierungen entwickelt: Software as a Service (SaaS), Platform as a Service (PaaS) und Infrastructure as a Service (IaaS). SaaS-Modelle stellen Anwendungen on demand über einen Web-Client bereit. PaaS bedeutet den Zugriff auf eine Computerplattform mit Betriebssystem, Middleware und/oder Datenbank, auf der Anwendungen erstellt und verwendet werden können. IaaS bedeutet die Bereitstellung einer Utility-Computing-Infrastruktur, die üblicherweise mit weiteren Ressourcen wie Hypervisor, Storage oder Networking ausgestattet ist und es ermöglicht, Plattformen und Anwendungen zu erstellen. Wird das Potential optimal genutzt, können Organisationen auf verschiedenste Art von Cloud Computing und seiner Skalierbarkeit, Agilität, schneller Marktreife und Kostenkontrolle profitieren.

## Software Asset Management

Software Asset Management ist das Lebensyklusmanagement des Softwarebestands einer Organisation. Ein Ziel ist dabei die Einhaltung der Lizenzvereinbarungen. Die Internationale Organisation für Standardisierung (ISO) hat in ihren globalen SAM-Standards (19770-1) die notwendigen Prozesse und Ziele definiert.

SAM gehört in jede Organisation, die Software verwendet. Die Implementierung von Cloud-Architekturen macht das noch dringender. Während effektives SAM diesen Prozess unterstützen kann, gefährdet ein falsches Vorgehen viele der finanziellen und anderen Vorteile von Cloud Computing.

## SAM in der Cloud

Geht eine Organisation den Schritt in die Cloud, muss ihr SAM-Programm den neuen Anforderungen angepasst werden. Zwar bleiben die Prinzipien die gleichen; es bestehen jedoch abweichende Lizenzrisiken und andere Effektivitäts-Anforderungen als in traditionellen IT-Umgebungen. Es muss Hardware und Software auch in der neuen Architektur in allen Nuancen erfassen.

In der Cloud betrifft SAM den Software- und den Service-Bestand. Die enorme Geschwindigkeit von Cloud-Umgebungen, wo Dienste innerhalb von Minuten bereitgestellt, konfiguriert, rekonfiguriert und freigegeben werden, zwingt das SAM, beinahe in Echtzeit zu agieren. Fehlerhafte Implementierungen stellen angesichts der neuen Möglichkeiten eine enorme Bedrohung dar und können von traditionellen IT- und SAM-Prozessen kaum erfasst werden. SAM muss für die Cloud neu konzipiert werden und Elemente wie versteckte Cloud-Service-Kosten oder zusätzliche Software-Lizenzkosten durch den Cloud-Einsatz in die Betriebskosten berücksichtigen sowie den Risiken durch neue Trends wie BYOD effektiv begegnen.

SaaS-Umgebungen sind für SAM ebenfalls eine Herausforderung. Organisationen können etwa Leidtragende eines Lizenzverstoßes des Cloud-Service-Providers (CSP) sein. Compliance-relevant sind sämtliche Szenarien unautorisierter Nutzung wie der Zugriff aus nicht erfassten Ländern, die gemeinsame Nutzung von Einzelaccounts oder die Bereitstellung von Zugriffsmöglichkeiten für externe Benutzer (Dienstleister, Kunden etc.) ohne entsprechende Erlaubnis. Manche SaaS-Lösungen arbeiten mit Plug-Ins und anderer nutzerseitiger Software, die ebenfalls ordnungsgemäß lizenziert sein muss. Die Vorstellung, dass Shelfware (brachliegende Software) in SaaS-Architekturen verschwindet, ist falsch. Schlechtes und ineffektives SAM kann in SaaS-Umgebungen zur Überbezahlung von ungenutzten Diensten führen und so die gesamte Organisation belasten.

Auch PaaS und IaaS haben ihre Fallstricke. So kann etwa Virtualisierung – die Basis dieser Modelle – in manchen Software-Lizenzvereinbarungen nicht vorgesehen sein. In anderen Fällen kann die Virtualisierung signifikante Kosten verursachen, wenn beispielsweise sämtliche physischen Prozessoren des Hardware-Unterbaus lizenziert werden müssen.
Die Erfassung von Hardware-Metriken in virtualisierten Umgebungen wird mit zunehmender Separierung zwischen Software und Hardware immer komplizierter. Die erfassbaren Daten könnten für manche Lizenzvereinbarungen nicht hinreichend sein. Außerdem ist es möglich, dass der Transfer von Lizenzen in die Cloud untersagt, beschränkt, zustimmungs- oder kostenpflichtig ist. Schließlich kann die spätere Rückübertragung der Lizenzen aus der Cloud unter Umständen nicht vorgesehen sein.

Werden herkömmliche Lizenzen für die lokale Nutzung von Software innerhalb eines Unternehmens für eine Nutzung in der Cloud verwendet, dann entbindet dies den Kunden weder von seinen lizenzrechtlichen Verpflichtungen gegenüber dem Hersteller, noch entbindet es ihn von der generellen Verantwortung einer Unterlizenzierung. Gleiches gilt auch in Fällen, in denen der CSP (Cloud Service Provider, der Dienstleister, welcher Cloud-Dienste anbietet) der Organisation Software in einer Art und Weise zugänglich macht, für die er keine ausreichenden Lizenzrechte besitzt: Die Risiko einer Urheberrechtsverletzung verbleibt auch bei der Organisation, weil sie die Software nutzt und von der unlizenzierten Nutzung profitiert. Abhängig von der konkreten vertraglichen Regelung wird der Organisation zwar ein Regressanspruch gegen den CSP zustehen, sofern dessen Verantwortlichkeit feststeht. Dieser mögliche Regressanspruch muss von der Organisation allerdings erst noch durchgesetzt werden.

Jedes SAM-Programm sollte in alle Facetten der Cloud-Strategie inklusive Design, Implementierung, Betrieb und Monitoring eingebunden sein. Nur so kann es dabei helfen, die vielfältigen Vorteile der Cloud zu nutzen und die Risiken zu minimieren.

## SAM in der Cloud — Aller Anfang ist schwer

SAM-Programme müssen der Cloud angepasst werden. Während die Details einer solchen Anpassung höchst vielfältig sein können, gibt es doch einige wichtige Leitlinien:

- SAM sollte vollständig in den Cloud-Management-Prozess integriert sein – beginnend mit der Planungsphase und dem Architektur-Design über Vertragsverhandlungen und -abschlüsse bis hin zum Monitoring der CSP-Compliance;
- SAM-Aktivitäten sollten den Kontakt zu den Herstellern der existierenden Software beinhalten, um die Regeln zum Cloud-Einsatz zu verstehen und gegebenenfalls neu verhandeln zu können;
- SAM-Verantwortliche sollten organisationsweite Cloud-Richtlinien initiieren, die beispielsweise den Bereitstellungsprozess, einzuholende Genehmigungen, Kontrollprozesse und nötige Bestandteile entsprechender Abschlüsse und ihrer Geschäftsbedingungen definieren;
- SAM sollte Zugriff auf sämtliche Cloud-Arrangements der Organisation haben (IaaS, PaaS, SaaS), diese Verträge prüfen und potentielle Lizenzrisiken einschätzen.

Dieses Whitepaper wurde im Auftrag der BSA von der Anglepoint Group, Inc verfasst. Anglepoint ist ein Dienstleister in den Bereichen SAM, Vertragstreue und Lizenzen für Fortune-500-Unternehmen. Der Gegenstand dieses Whitepapers unterliegt ständigen Veränderungen: neue Risiken und neue Lösungen sind an der Tagesordnung. Diese Veröffentlichung ist somit weder eine erschöpfende Behandlung des Themas noch ersetzt sie eine professionelle Beratung.

## Die wichtigsten Punkte

- Cloud Computing beseitigt Lizenzprobleme nicht, sondern schafft neue. Diesen Herausforderungen kann man mit effektivem Software Asset Management begegnen;
- Software Asset Management ist entscheidend sowohl für Unternehmen auf dem Weg in die Cloud als auch für solche mit traditionellem Software-Bestand;
- Auch in der Cloud verfolgt SAM die gleichen Ziele – es ändert sich aber die Herangehensweise;
- SAM sollte integraler Bestandteil jeder Unternehmens-Cloud-Strategie und des Implementierungsplans sein; die vollständige Integration in den Cloud-Management-Prozess ist essentiell;
- SAM sollte fortlaufend angepasst werden, um den Cloud-Management-Prozess als ganzen zu managen. Richtlinien und automatisierte Kontrollen sind eine geeignete Antwort auf die dynamische Echtzeitrealität der Cloud;
- Traditionelle Software-Lizenzvereinbarungen müssen vor dem Schritt in die Cloud genau überprüft werden, um Compliance-Schwierigkeiten zu vermeiden. Es ist dringend zu empfehlen, hier eng mit dem jeweiligen Hersteller zusammenzuarbeiten;
- BYOD kann ein zusätzliches Risiko darstellen;
- Software as a Service birgt Herausforderungen in den Bereichen unautorisierte Benutzung und Shelfware.

# Einführung: Cloud-Technologien

## Es gibt zwar eine Basisdefinition von Cloud Computing. Doch Technologien, Plattformen und Ansätze unterliegen einem ständigen Wandel.

Das amerikanische National Institute of Standards and Technology (NIST) definiert Cloud Computing[1] als „ubiquitären, einfachen on-demand-Netzwerkzugriff auf einen Pool konfigurierbarer Computerressourcen, die schnell und mit nur minimalem Verwaltungsaufwand und Provider-Interaktion bereitgestellt werden können“.

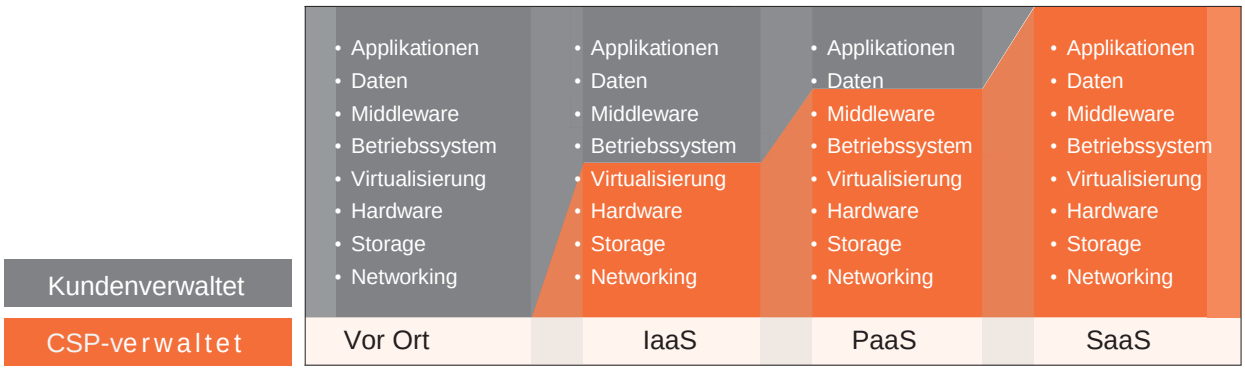
Die wachsende Beliebtheit des Cloud Computing ist auf eine Konvergenz verschiedener Trends zurückzuführen: die Reife von Virtualisierungs- und -Management-Technologien; Big Data (Sammlung, Speicherung, Verwaltung und Analyse sehr großer Datenmengen); die zunehmende Verfügbarkeit bezahlbarer Breitbandnetzwerke mit hohen Kapazitäten sowie die Verbreitung mobiler Geräte mit Netzwerkzugriff.

## Cloud-Service-Modelle

Cloud-Computing-Anbieter nutzen verschiedene Modelle, oft auch in Kombination. Laut NIST sind die folgenden am meisten verbreitet:

| | |
|---|---|
| *Software as a Service (SaaS):* | Die Nutzung von Applikationen des Dienstleisters auf einer Cloud-Infrastruktur. Die Anwendungen können von verschiedenen Geräten genutzt werden, entweder über eine Thin-Client wie den Browser (z.B. bei webbasierte E-Mail) oder über eine Programmschnittstelle. Der Kunde hat keinen Einfluss auf die zugrunde liegende Cloud-Infrastruktur aus Netzwerk, Servern, Betriebssystemen, Storage oder sogar individuelle Anwendungsoptionen. Unter Umständen ist lediglich die begrenzte Wahl nutzerspezifischer Programmeinstellungen möglich. |
| *Platform as a Service (PaaS):* | Die Nutzung selbst kreierter oder erworbener Anwendungen auf einer zur Verfügung gestellten Cloud-Infrastruktur. Es muss Kompatibilität von Programmiersprachen, Libraries, Diensten und Werkzeugen bestehen. Auch hier hat der Kunde keine Kontrolle über die Infrastruktur. Sein Verwaltungszugriff beschränkt sich auf die eingesetzten Anwendungen und möglicherweise auf bestimmte Konfigurationen. |
| *Infrastructure as a Service (IaaS):* | Die Nutzung fundamentaler Ressourcen wie Processing, Storage oder Netzwerke. Der Kunde kann selber verschiedene Softwarelösungen – Betriebssysteme und Applikationen – einsetzen. Er kontrolliert dabei nicht die zugrundeliegende Infrastruktur, sonder lediglich Betriebssysteme, Storage und die eingesetzten Anwendungen; hat aber eventuell eingeschränkten Zugriff auf einzelne Netzwerkkomponenten wie etwa Host Firewalls. |

Traditionell umfassen IT-Architekturen acht Elemente. Diese Übersicht zeigt, wie die Verantwortung für diese Komponenten im Rahmen der drei Cloud-Modelle zwischen Kunde und CSP verteilt ist:



## Cloud-Deployment-Modelle

Cloud-Technologien können mit verschiedenen Modellen zugänglich gemacht werden. Nach dem NIST sind dies die Häufigsten:

| | |
|---|---|
| *Private Cloud:* | Die Cloud-Infrastruktur für den exklusiven Zugriff eines einzelnen Kunden. Innerhalb dieses Kunden gibt es mehrere interne Kunden (z.B. einzelne Abteilungen). Eigentum und Verwaltung kann beim Kunden, Dritten oder beiden in beliebiger Kombination liegen; die Cloud kann vor Ort oder extern gehostet werden. |
| *Community Cloud:* | Die Cloud-Infrastruktur steht einem definierten Nutzerkreis mit ähnlichen Interessen (z.B. Sicherheit, Compliance) aus verschiedenen Organisationen zur Verfügung. Sie kann von einer dieser Organisationen oder einem Dritten besessen, verwaltet und betrieben werden; sie kann vor Ort oder extern gehostet werden. |
| *Public Cloud:* | Die Cloud-Infrastruktur ist auf öffentliche Benutzung ausgelegt. Sie kann von einem Unternehmen, einer Universität, einer Behörde oder einer Kombination davon besessen, verwaltet und betrieben werden und wird üblicherweise in deren Räumlichkeiten gehostet. |
| *Hybrid Cloud:* | Die Cloud-Infrastruktur setzt sich aus zwei Infrastrukturen (Private, Community, Public) zusammen, die separate Einheiten bleiben und durch standardisierte oder proprietäre Technologie gebündelt werden. So kann Daten- und Anwendungsportabilität erreicht werden etwa, um die Last zu verteilen. |

Eine beliebte und rasch wachsende Variante der Public Cloud ist die Personal Cloud. Sie stellt Dienste wie Social Media, persönliche E-Mail, Dokumenterstellung und Foto-, Musik- oder Videobearbeitung für individuelle Kunden bereit.

# Einführung: Software Asset Management

## Die Information Technology Infrastructure Library (ITIL) definiert Software Asset Management[2] folgendermaßen:

> Die Gesamtheit von Infrastruktur und Prozessen, die für die effektive Verwaltung, Kontrolle und Erhaltung des Software-Bestands einer Organisation während des gesamten Lebenszyklus notwendig ist.

Diese Standarddefinition wird erweitert durch eine funktionale:

> SAM ist das effektive Management dessen, was eine Organisation mit Software tut oder nicht tut. Es sind die Prozesse und funktionalen Ressourcen zur Verwaltung des Softwarebestands während der fünf Phasen ihres Lebenszyklus (Planung, Beschaffung, Einsatz, Wartung und Stilllegung).

Software-Lizenzmanagement (SLM) ist die Anwendung von SAM auf Lizenzierungsfragen (Erfassung und Verwaltung von Berechtigungen und deren Inanspruchnahme).

Software License Compliance (SLC) ist eine Untereinheit von SAM und beschreibt die Sicherstellung der Lizenztreue (Compliance). Lizenz-Compliance ist ein Kernelement von SAM. Für optimale Ergebnisse sollten Organisationen regelmäßig ihre Berechtigungen unter der Lizenzvereinbarung mit ihrem tatsächlichen Bedarf vergleichen. Diese Informationen ergeben komplette und akkurate Daten zum Software-Einsatz inklusive einer Zählung der Lizenzen (die sich je nach Produkt unterscheidet), der Anwendung der Lizenzregeln, Nutzungsrechte und andere Informationen wie etwa Bündelungsregeln. Informationen über die Lizenzberechtigungen ergeben sich aus den vollständigen Beschaffungsnachweisen, Lizenzvereinbarungen und weiteren.

Wie angedeutet, sind die folgenden Punkte für SAM charakteristisch:

- SAM ist eine Geschäftspraktik, die Menschen, Prozesse und Technologien beinhaltet;
- SAM besteht aus Verwaltungsprozessen und funktionalen Ressourcen. Werkzeuge können zur Vereinfachung oder vereinzelt sogar zur Automatisierung beitragen; der Einsatz kann jedoch nur effektiv sein, wenn er effektiv geplant ist;
- SAM beschäftigt sich mit Software, für die eine Organisation Richtlinien erlässt. Es geht also nicht nur um Desktop- sondern noch viel mehr um Server-Software: Dort sind Kosten und operationaler Einfluss der Software am höchsten. Interessanterweise geht es auch bei der Cloud um Software auf Servern. SAM kann darüber hinaus auch die Software auf Telefonen, Switches, Druckern etc. umfassen;
- SAM ist multidisziplinär. Effektivität kann nicht in einer isolierten Abteilung erzielt werden, sondern benötigt Kollaboration zwischen verschiedenen Bereichen wie IT, Buchhaltung, Rechtsabteilung und Personalabteilung.

Effektives SAM liefert konsistente und wiederholbare Ergebnisse. Auf dieser Faktenbasis ergibt sich die größtmögliche Kenntnis der vorhandenen und der tatsächlich genutzten Berechtigungen sowie deren Verwendungsort und -Art. Davon profitieren SLM, SLC, Informationssicherheit, Kontinuitäts-, Change- und Konfigurationsmanagement sowie Lizenz-Compliance.

Effektive **Informationssicherheit** benötigt die Identifikation des gesamten Hardware- und Software-Bestands. Sein Einsatz muss autorisiert sein, markenecht und mit der aktuellen, originalen Sicherheitskonfiguration versehen sein. **Kontinuitätsmanagement** kann nur effektiv sein, wenn bekannt ist, welche Teile des Bestands welche Geschäftsprozesse unterstützen und welche Abhängigkeiten bestehen. Außerdem muss im Schadensfall jeder Server rekonstruierbar sein - bis hin zur korrekten Version und dem aktuellen Patch. Im Rahmen eines effektives Change- und Konfigurationsmanagements muss sichergestellt sein, dass keine unautorisierten Änderungen an Konfigurationen vorgenommen werden, was wiederrum das Wissen voraussetzt, über welche Rechner eine Organisation wo und in welchen Konfigurationen verfügt.

## SAM-Standards

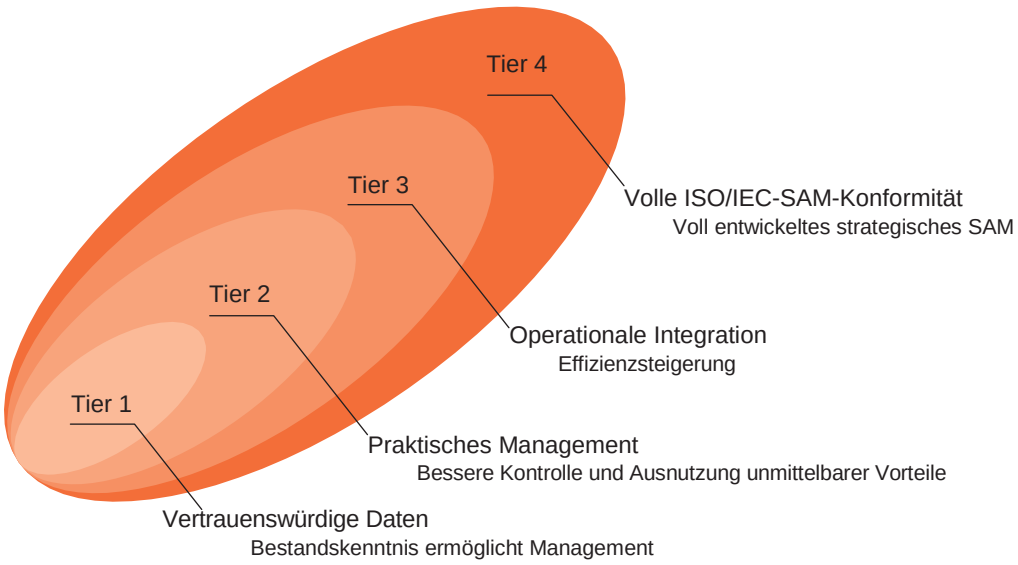
Die International Organization for Standardization (ISO) ist die größte und anerkannteste Standardisierungsorganisation. Die Familie ISO 19770[3] ist der einzige globale SAM-Standard.

### 19770-1 SAM-Prozesse

Dieser Standard wurde 2006 veröffentlicht und 2012 überarbeitet. Er behandelt Prozesse, definiert Stufen der Erfüllung und klassifiziert vier ergebnisorientierte Konformitätslevel (Tier).

Der **BSA SAM Advantage Course**[4] ist der erste SAM-Kurs nach ISO/IEC 19770-1:2012.

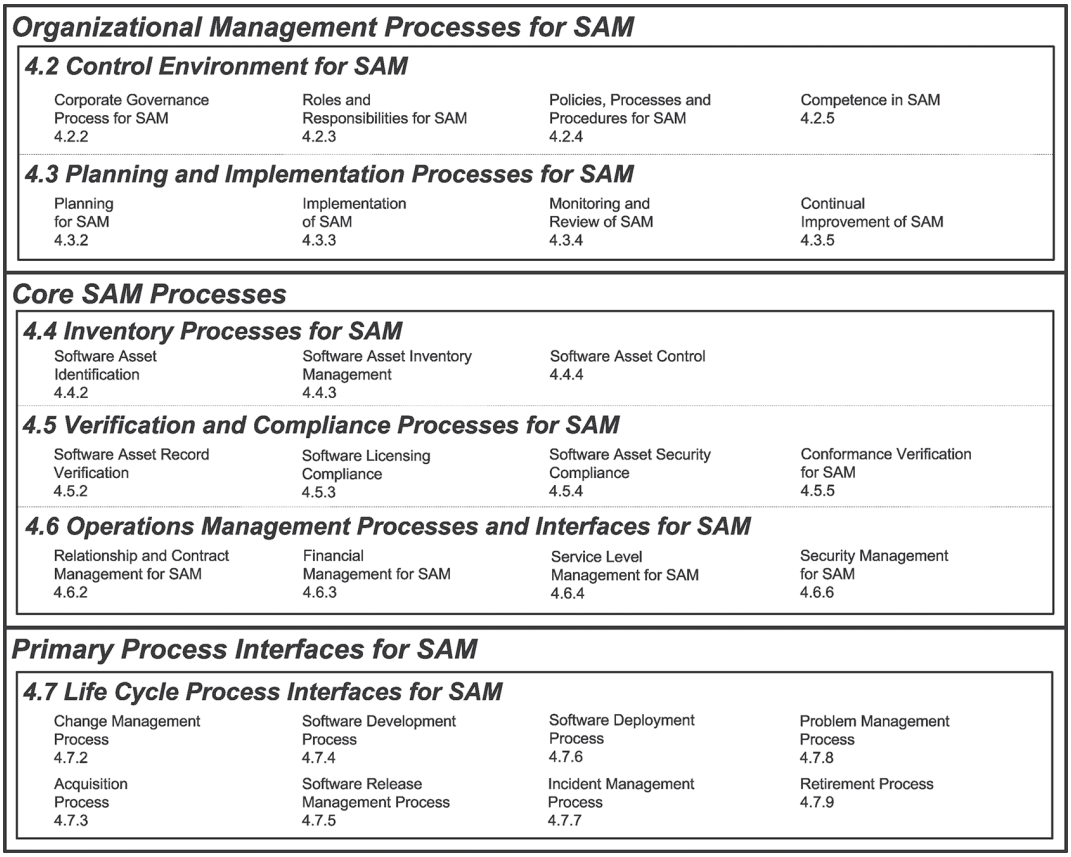
ISO 19770-1 TIERED ASSESSMENT FRAMEWORK




ISO/IEC 19770-1 identifiziert integrierte SAM-Prozesse sowie das klassifizierte Vorgehen bei ihrer Implementierung. Die 27 Prozesse sind unterteilt in drei Hauptkategorien und sechs Untergruppen. Der vierstufige Implementierungsansatz basiert auf der Erreichung spezifischer Konformitätsergebnisse durch diese Prozesse.

ISO/IEC 19770-1 ist auf jede Software sowie sämtliche Technologiearchitekturen anwendbar. Es ist gleichermaßen relevant für eine Produktivitätsanwendung auf einem Laptop wie für eine SaaS-Applikation aus einer Cloud-Umgebung.

ISO 19770-1 SAM PROCESSES FRAMEWORK




## 19770-2 Software-ID-Tags

ISO/IEC 19770-2 fokussiert Software-ID-Tags (SWID): Der 2009 erstmals veröffentlichte Standard schafft einen Rahmen, der die vollständige und akkurate Identifikation sämtlicher installierter Software ermöglicht. Hersteller und Endnutzer profitieren davon gleichermaßen.

19770-2 definiert sowohl zwingende als auch optionale Elemente innerhalb eines SWID-Tags. Diese nutzen standardisierte XML, die bei der Installation der Software an vorher festgelegten Orten auf Maschinen platziert werden.

TagVault[5] (tagvault.org) ist eine Non-Profit-Organisation, die mit einem zentralen Tag-Archiv eine Vereinfachung der 19770-2-Implementierung anstrebt.

Zahlreiche Software-Hersteller haben sich bereits angeschlossen und versehen neue Software mit SWID-Tags. Für Altsysteme können Organisationen eigene oder Drittanbieter-Tags nutzen.

Die Nutzung von SWID-Tags ermöglicht es, die in der Organisation eingesetzte Software schnell und akkurat zu identifizieren. In IaaS- und PaaS-Umgebungen können selbst erstellte SWID-Tags dabei helfen, eigene Software von der des CSP oder von weiteren Kunden zu unterscheiden. Diese Tags spielen eine immer größere Rolle für das SAM und können besonders in der Cloud zunehmend relevant werden.

**Künftige ISO SAM-Standards:** ISO entwickelt derzeit mehrere Standards, etwa 19770-3 für Lizenz-Tags und 19770-7 für die Verwaltung von 19770-2- und 19770-3-Tags.

# SAM in der Cloud – Grundsätzliche Überlegungen

In Bezug auf Software-Lizenzierung hat jedes Cloud-Service-Modell seine eigenen Risiken. Der folgende Abschnitt behandelt notwendige Erwägungen, ohne zu sehr ins Detail zu gehen.

## Anpassung von SAM an die Cloud

Cloud Computing schließt die Notwendigkeit von SAM nicht aus. Eine Cloud-Umgebung ist lediglich eine andere Infrastruktur, in der SAM-Prozesse effektiv vonstattengehen müssen. Organisationen sollten ihre Umsetzung der 27 Prozessbereiche von ISO 19770-1 so anpassen, dass alle Nuancen der Software und Architektur in ihrer Cloud-Umgebung erfasst werden. So wie Organisationen den Unterschied zwischen physischen und virtuellen Umgebungen berücksichtigen müssen, gilt es auch, für die Cloud optimale Praktiken zu finden.

Organisationen müssen Cloud Computing in ihren Richtlinien und Prozessen gezielt behandeln, um dem ISO 19770-1 zu genügen. Einige wichtige Überlegungen bei einer SAM-Implementierung in Cloud-Umgebungen sind:

- *Die Natur des Software-Bestands verändert sich.* Traditionelles SAM befasst sich lediglich mit dem Lebenszyklusmanagement des zugrundeliegenden Software-Bestands. Die Cloud erweiterte das SAM um die Cloud-Services selber, die zu einer Art Bestand werden, der verwaltet werden will. Da bestimmte SAM-Aspekte nicht beim Kunden liegen, sondern vom CSP zur Verfügung gestellt werden, umfasst SAM auch die Einhaltung der SLA-Vereinbarungen (Service Level Agreement) und der übrigen anwendbaren Regeln. Diese Anforderungen zwingen SAM-Programme zu neuen Ansätzen, neuen Fähigkeiten und neuen Tools.

- *Echtzeit-SAM.* Einer der Vorzüge der Cloud ist ihre Agilität, ihre Geschwindigkeit. Cloud-Dienste können mit wenigen Clicks erstellt und zugänglich gemacht werden. Traditionelle SAM-Prozesse sind dagegen oft von längeren Lebenszeiten und damit von einer größeren Zeitspanne für Planung, Beschaffung, Problemfindung etc. ausgegangen. Dies muss nun an eine beinahe in Echtzeit agierende Umgebung angepasst werden. Es müssen Prozesse definiert werden, die rasche Reaktion ermöglichen. Detaillierte, unternehmensweite Richtlinien für Verträge, Einsatz und Verwaltung können diesen Prozess unterstützen.

- *Dezentralisierung.* Cloud-Services, besonders SaaS, sind grundsätzlich einfach zu implementieren und benötigen oft kein größeres IT-Wissen oder besondere Ressourcen. Deshalb stellen viele Organisationen fest, dass ihre Angestellten die üblichen IT-Beschaffungsprozesse bei der Nutzung von Cloud-Diensten umgehen. Oftmals sprechen SaaS-Anbieter mittlerweile direkt die potentiellen Anwender an, statt über den Einkauf zu gehen. Cloud-Services werden üblicherweise als Betriebskosten veranschlagt und unterliegen deshalb häufig nicht den strengeren Anforderungen an Kapitalaufwendungen. Sie können oft direkt per Kreditkarte bezahlt werden, ohne durch mehrere Freigabestufen zu gehen. Aus diesen Gründen erfahren IT- und SAM-Verantwortliche meist erst nachträglich (wenn überhaupt) von Cloud-Implementierungen und haben deshalb auch keine Kontrolle über die Abschlüsse. Daraus ergibt sich eine Vielzahl von Herausforderungen:

  - *Verträge.* SAM, IT und Beschaffung sind nicht ausreichend in den Vertragsabschluss involviert;

  - *Lizenzen.* Ohne SAM-Beteiligung bei Design, Vertrag und Monitoring entstehen Lizenzrisiken;

  - *Speicherort.* Datenstandorte können unbekannt sein. Dieses Kontrollminus kann zu Risiken für Privatsphäre, Informationssicherheit und Unternehmenskontinuität führen;

  - *Abhängigkeiten.* Ohne effektive Kontrolle sind auch Szenarien denkbar, in denen Geschäftsprozesse von einer nicht genehmigten Cloud-Lösung abhängig werden;

  - *Kosten.* Nutzer können oftmals problemlos weitere Funktionen freischalten oder kostenpflichtig ihr Speicherlimit überschreiten. Ohne IT-Kontrolle können derartige Kosten oft nicht einmal final beziffert, geschweige denn gesteuert oder korrekt verbucht werden. Dies hat dramatische Auswirkungen auch auf die Finanztransparenz.

- *TCO in der Cloud.* Eines der Hauptanliegen jedes SAM-Programms ist es, die Gesamtkosten (Total Cost of Ownership – TCO) des Software-Bestands und seiner Verwaltung nachzuvollziehen. Für klassische Lizenzen sollte dies bereits der Fall sein. Die Cloud ist jedoch eine andere Umgebung mit anderen Verträgen und Vorgehensweisen, auf die sich eingestellt werden muss. Vereinbarungen, die simpel erscheinen, können eine Vielzahl direkter, indirekter und versteckter Kosten mit sich bringen, etwa für die Cloud-Migration, Integration, die Notwendigkeit eines Premium-Supportlevels, zusätzlichen Storage-Bedarf, steigende Wartungskosten und so weiter.
  Ferner kann der hohe Virtualisierungsgrad der Cloud zu weiteren Kosten führen, da er unter herkömmlichen Lizenzbedingungen nicht immer unterstützt wird.

## Bring Your Own Device

Einer der Hauptvorteile von Cloud Computing ist die Zugriffsmöglichkeit über das Internet. Dieses Merkmal konvergiert mit einem weiteren IT-Trend: BYOD – Unternehmen erlauben ihren Mitarbeitern, von ihren privaten Endgeräten (Laptops, Tablets, Smartphones) auf Geschäftsinformationen und -applikationen zuzugreifen. Dieses Konzept passt zum Cloud-Zugriff, der ebenfalls prinzipiell von überall aus möglich ist. Viele SaaS-Anbieter haben spezielle Apps für BYOD-Geräte im Programm. Aus SAM-Sicht ergeben sich die folgenden Zusatzrisiken:

- *Lizenzen für mobile Zugriffs.* Der Zugriff auf Cloud-Software von mobilen Geräten muss eine vollständige Lizenzbasis haben. In den Lizenzbedingungen kann BYOD-Zugriff ausgeschlossen oder mit zusätzlichen Kosten belegt sein.

- *Sicherheitsrisiken.* Angesichts der Tatsache, dass in BYOD-Szenarien die Organisation keine Kontrolle über Sicherheitskonfigurationen oder die Verbindung in die Cloud (denkbar ist etwa auch persönliches WLAN) hat, ergeben sich deutliche Sicherheitsbedenken.

- *Personal Cloud und Einsatz persönlicher Apps für Geschäftszwecke via BYOD.* BYOD erlaubt den einfachen Zugriff auf persönliche Apps in Personal-Cloud-Diensten (etwa Produktivitätsanwendungen wie Notizen). Durch die Verwendung des privaten Geräts bei der Arbeit ist die Chance groß, dass solche Anwendungen auch für Arbeitszwecke verwendet werden. Dies kann jedoch im Widerspruch zu deren Lizenzbestimmungen stehen, was ein Risiko für den Nutzer und für das Unternehmen eröffnet. Außerdem können auf diesem Weg Unternehmensdaten in private Clouds gelangen, wo sie der Kontrolle der Organisation entzogen sind und ein eigenständiges Sicherheits- und Datenschutzrisiko darstellen.

- *Risiko illegale Software und BYOD.* Organisationen können kaum kontrollieren, welche Software ihre Angestellten auf persönlichen Geräten laden und installieren, woher diese Software stammt und ob sie ordnungsgemäß lizenziert ist. Da stets die Gefahr raubkopierter Programme besteht, sind Organisationen hier einem deutlichen Risiko ausgesetzt. Nutzt der Angestellte diese Software zu Geschäftszwecken, können darüber hinaus Compliance-Probleme entstehen.

## Vollständige Compliance

Viele Organisationen haben zusätzlich zu ihren eigenen Datensicherheitsvorgaben auch gesetzliche Bestimmungen zu beachten. Dies kann unter anderem die Notwendigkeit regelmäßiger Datenschutznachweise mit sich bringen.

Eine dieser Bestimmungen ist PCI DSS, ein Sicherheitsstandard für alle Organisationen, die mit Kartendaten arbeiten, seien es Kredit-, Prepaid-, Giro- oder andere Karten. Um eine PCI DSS Zertifizierung zu erlangen und zu halten, müssen Organisationen jährliche Prüfungen durchführen. Um diese Prüfung zu durchlaufen muss eine Organisation Details ihrer Infrastruktur kennen (Hard- und Software, Netzwerk, Firewall etc.). Bei Organisationen mit großen Datenvolumina sind Begehungen der Standorte vorgeschrieben. Ohne umfassende Planung kann der Schritt in die Cloud die Einhaltung dieser Standards erheblich erschweren.

Die folgenden Gesetze ziehen eine Vielzahl zusätzlicher Bestimmungen nach sich, die Organisationen in Bezug auf Datenstandort, -Zugang und -Sicherheit zu beachten haben:

- USA:
  - Sarbanes-Oxley (SOX);
  - Health Insurance Portability and Accountability Act (HIPAA);
  - Electronic Records and Electronic Submissions CFR 21 part 11;
  - Financial Modernization Act von 1999;
  - Federal Desktop Core Configuration (FDCC);
  - USA PATRIOT Act und US Presidential Executive Order 13103.
- Andere:
  - Europäische Union — Datenschutzrichtlinie und zusätzliche Gesetze in Mitgliedsstaaten;
  - Australien — Corporate Law Economic Reform Program Act 2004 (CLERP9);
  - Malaysia — Personal Data Protection Act 2010;
  - Indien — The Institutes of Technology (Amendment) Act und Clause 49 des Listing Agreement to the Indian Stock Exchange;
  - Südafrika — King Report on Corporate Governance.

Datenschutz ist eines der zentralen Probleme des Cloud Computing. Die EU-Richtline zum Datenschutz verbietet etwa den Transfer persönlicher Daten in Nicht-EU-Länder, die keinen im Sinne der EU adäquaten Datenschutz garantieren. Um den Unterschied zum US-amerikanischen Ansatz zu überbrücken, wurde ein Mechanismus geschaffen, der es Organisationen, die in den USA aktiv sind, ermöglicht, der EU-Richtlinie zu entsprechen. Das US-Handelsministerium hat deshalb in Zusammenarbeit mit der Europäischen Kommission das Safe Harbor-Abkommen geschaffen. Organisationen, die bestimmte Kriterien der Datensicherheit erfüllen, können ihm beitreten. Diese umfassen Benachrichtigung über die Speicherung persönlicher Daten, Klarheit über ihre Verwendung und diverse Schutzvorschriften.

Safe Harbor stellt jedoch nur eine von mehreren Möglichkeiten des legalen Datentransfers dar. Organisationen müssen deshalb möglicherweise auch andere Optionen in Betracht ziehen.

Diese komplexen Anforderungen beeinflussen die Ausgestaltung von SAM-Programmen deutlich. Egal, um welche Art Cloud-Dienst es geht, immer muss die Regulierungsinstanz einbezogen werden – beinahe wie eine externe Erweiterung des eigenen Teams. Dies zu vernachlässigen oder gar zu ignorieren kann zu unnötigen Zusatzrisiken und -kosten führen, die die Vorteile der Cloud überlagern können.

## SAM als Cloud-Treiber

Oft wird die Fähigkeit eines effektiven SAM-Programms übersehen, Strategien zu formen. Detailliertes Wissen über verfügbare Software, Hardware und Infrastruktur kann ein starkes Fundament für kritische Wachstums-, Akquisitions- und andere strategische Entscheidungen sein.

Cloud Computing ist eine dieser Strategien, für die das SAM essentielle Informationen liefern kann. Das Verständnis der momentanen Geschäftsumgebung (Hard- und Software) ist entscheidend dafür, ob Cloud Computing wirtschaftlich sinnvoll ist.

Niemand kann etwas optimieren, worüber er nichts weiß. Ob es um die Virtualisierung vor Ort, den Schritt in eine Private Cloud oder eine Public Cloud (IaaS, PaaS, SaaS) geht: Jede Organisation muss ihren Bestand kennen, wissen, wo sich die Ressourcen im Einzelnen befinden, wie sie konfiguriert sind, wer sie wozu und wie nutzt, wie die Lizenzlage (auch im Hinblick auf eine mögliche Cloud-Migration) und wie hoch der TCO ist.
Nur mit diesen Informationen kann der nötige ROI erfasst werden, der Virtualisierung oder Cloud Computing erst zum Erfolg machen kann. Kurz: SAM ist eine Kernkompetenz für den Schritt in die Cloud.

# Software as a Service – Überlegungen aus SAM-Sicht

Software as a Service ist ein Abonnement-Service, auf den meist über den Webbrowser zugegriffen wird. Bekannte Beispiele sind etwa Salesforce.com, Microsoft Office 365, Google Apps oder NetSuite.

SaaS wird typischerweise im Rahmen eines von vier Geschäftsmodellen oder einer Kombination daraus angeboten:

- *Zeitbasiert.* Das am weitesten verbreitete Modell erlaubt den Zugriff für einen bestimmten Zeitraum gegen Zahlung einer Gebühr. Ihre Höhe kann je nach Umfang der Dienste variieren.
- *Nutzungsbasiert.* Ein derzeit wenig genutztes Modell kalkuliert die Gebühr aus Nutzungsdaten wie der Anzahl der Anmeldungen, der Dauer der Sitzungen, der Transaktionszahl, des Speichervolumens oder einer Kombination daraus.
- *Erfolgsbasiert.* Ein ebenfalls seltenes Modell basiert auf tatsächlich erzielten Resultaten: man stellt beispielsweise einen bestimmten Prozentsatz des Gewinns pro Transaktion in Rechnung oder kalkuliert aus dem Gesamtergebnis des Kunden.
- *Anzeigenfinanziert.* Gerade in der Personal Cloud ist häufig das kostenfreie Modell anzutreffen, das über Anzeigen finanziert wird.

Eine weit verbreitete Fehleinschätzung besagt, dass SaaS keine Lizenzrisiken aufwirft und deshalb aus dem SAM heraus genommen werden kann. Je nach CSP und individueller Vereinbarung variieren die Risiken zwar, doch es gibt einige, die weit verbreitet sind:

- *IP-Verstöße:* Der SaaS-Anbieter kann bewusst oder unbewusst gegen das Urheberrecht eines Dritten verstoßen. Existiert keine vertragliche Vereinbarung, die den CSP verpflichtet, sämtliche Haftungsrisiken auf sich zu nehmen, können diese auch den Kunden als primären Nutznießer treffen. Operiert der CSP in einem anderen Land als der Kunde, greifen möglicherweise schwächere IP-Gesetze. Zuletzt kann ein solches Risiko auch zur Nichtverfügbarkeit der Dienste führen.

- *Clientseitige Software-Komponenten:* Entgegen einer weit verbreiteten Annahme ist es durchaus möglich, dass SaaS-Lösungen eine clientseitige Code-Installation benötigen. Dies kann in Form eines Browser-Plugins, Applets, Agents oder sogar einer vollständigen Suite (etwa MS Office Professional Suite bei Microsoft Office 365) geschehen. Der Kunde muss erstens vollständig lizenziert sein und dies bei einem Audit auch nachweisen können; und zweitens diese Bestände genauso verwalten wie andere: Sie dürfen nur im zulässigen Umfang und gemäß ihrer Nutzungsbestimmungen installiert werden.

  *Beispiel: Eine Organisation nutzte als Teil ihres Standard-PC-Images eine clientseitige Softwarekomponente ihres SaaS-Dienstes. Dies führte zu einer deutlich häufigeren Nutzung als Nutzer im Rahmen des SaaS-Vertrag autorisiert waren.*

- *Unautorisierte Nutzung:* SaaS unterliegt typischerweise verschiedenen Beschränkungen. Diese Grenzen sind oft nicht verhandelbar. Vollständige Compliance setzt die korrekte Kontrolle voraus. Folgende Maßnahmen sind beispielsweise denkbar:

  - Geographische Beschränkungen, die etwa nur Angestellten innerhalb der USA den Zugriff erlauben (wo andere Preismodelle greifen als in anderen Ländern).
  - Beschränkungen des Account-Sharing.

    *Beispiel: Ein Abteilungsleiter stellt zehn Angestellten seine Logindaten für eine Schulungssoftware zur Verfügung.*
  - Beschränkungen des Zugriffs durch System-Accounts (die den Zugriff durch ein anderes System statt eines echten Anwenders betreffen).
  - Beschränkungen beim Zugang für Dritte (etwa Dienstleister oder Partner des Kunden), die im Extremfall die Nutzung der SaaS-Lösung komplett unterbinden können.
  - Beschränkungen der Bereitstellung von Reports und Informationen an Nicht-Lizenznehmer. Denkbar sind Situationen, in denen ein individuell lizenzierter Nutzer einen Bericht generiert und ihn dem gesamten Team schickt.

Manche SaaS-Anbieter nutzen Analyse-Tools zur Aufdeckung unautorisierter Nutzung. Dabei wird etwa Folgendes analysiert:

- Gleichzeitige Mehrfachnutzung eines Accounts;
- IP-Adresse mit Länderinformation;
- Uhrzeit des Zugriffs;
- Daten- und Transaktionsvolumen;
- Vergleich des Kundenprofils mit öffentlich zugänglichen Informationen (etwa die Anzahl der Beschäftigten eines Unternehmens);
- Erkennung ungewöhnlicher Nutzungsmuster durch den Vergleich von Kundenprofilen mit solchen aus derselben Branche.

- *Shelfware:* Entgegen einer weit verbreiteten Auffassung ist die Existenz von Shelfware auch mit SaaS möglich und nicht einmal selten. Dies liegt hauptsächlich daran, dass beinahe alle derzeitigen SaaS-Modelle nicht auf pay-per-use-Regeln basieren, sondern auf einer Vertragslaufzeit, etwa auf ein Jahr. Kosten und tatsächliche Nutzung können deshalb divergieren. Endnutzerorganisationen stellen möglicherweise fest, dass sie für mehr Leistung zahlen als sie benötigen. Dies kommt typischerweise bei neuen Verträgen vor oder wenn nur wenige Nutzer die neuen Möglichkeiten ausschöpfen. Auch im Falle einer Stellenreduktion werden die Zahlungen an den SaaS-Provider zunächst gleich hoch bleiben.

- *Skaleneffekt:* Einige traditionelle Enterprise-Software-Lizenzmodelle – etwa solche, die auf Hardwaremetriken basieren – berücksichtigen Skaleneffekte. Der Endnutzer kann unter Umständen die Softwarenutzung erhöhen, ohne zwingend auch die Kosten zu steigern. Beim Übergang zu nutzerbasierten SaaS-Modellen kann dieser Vorteil wegfallen. Die Organisation käme nicht in den vollen Genuss der Einsparungen. Zum Beispiel kann eine Organisation höheren Anforderungen an die Software im Rahmen ihres Lizenzmodells nicht mehr kostengünstig mit einem Hardware-Upgrade begegnen (Prozessorgeschwindigkeit, Memory, Netzwerkgeschwindigkeit). Stattdessen erhöht jeder zusätzliche Nutzer direkt die Kosten im Vertragszeitraum, selbst wenn er die Software nur für kurze Zeit nutzt.

- *Untervergabe und SaaS:* Eine weitere Komplexitätsschicht ergibt sich aus der Praxis vieler Anbieter, ihre Dienste über weitere Anbieter (z.B. IaaS/PaaS) zur Verfügung zu stellen. So kann ein Webanbieter von SaaS etwa die cloudbasierte Infrastruktur von Amazon nutzen. Einige der angesprochenen Probleme hängen mit diesen zusätzlichen Providern zusammen oder ergeben sich erst daraus. Jede Organisation muss wissen, welche Ansprüche sie gegenüber dem gesamten SaaS-Ökosystem geltend machen kann.

# SAM und Virtualisierung/ Private Cloud

## Alle Cloud-Technologien und Einsatzmethoden abgesehen von SaaS basieren im Wesentlichen auf Virtualisierungs-Technologien.

Virtualisierung ist der Einsatz eines virtuellen statt physischen IT-Elements wie Hardware oder Storage. Die Technologie existiert bereits seit Jahrzehnten und hat ihren Anfang bei Mainframe-Computern. In den vergangenen Jahren hat die Virtualisierung alle Bereiche der IT erreicht. Alle Technologien der Virtualisierung zu beschreiben würde hier den Rahmen sprengen, aber ohne ein grundlegendes Verständnis ist keine Diskussion der Herausforderungen von SAM in der Cloud möglich.

Virtualisierung umfasst ein bestimmtes Maß an Trennung von Soft- und Hardware. Traditionell ist dieses Verhältnis direkt und unmittelbar: ein Betriebssystem (OS) oder ein bestimmtes Software-Produkt pro Element der Hardware. Deswegen sind auch heute noch die Lizenzmodelle am weitesten verbreitetet, die auf Hardware basieren (zum Beispiel Lizenzierung pro Prozessor), denn das ist am einfachsten zu messen.

Im Gegensatz dazu gilt bei der Virtualisierung ein unsymmetrisches Verhältnis von Hardware zu Software. Auf einer einzelnen Hardware können jetzt mehrere virtuelle Rechner laufen, von denen jeder sein eigenes Betriebssystem und Applikationen hat. Die Ressourcen der Hardware wie Prozessor oder Speicher werden oft flexibel zwischen den verschiedenen Betriebssystemen verteilt, um Lastspitzen besser auffangen zu können.

Virtualisierung stellt die Hardware-basierte Lizenzierung von Software damit vor Probleme, vor allem, da viele Lizenzverträge zu einer Zeit geschlossen wurden, als Virtualisierung noch nicht berücksichtigt wurde. Die verschiedenen Hersteller gehen auf unterschiedliche Art und Weise mit der Messung von Hardware in virtuellen Umgebungen um. Viele fordern den Kunden auf, die maximal mögliche Hardware-Konfiguration als Basis der Lizenzierung heranzuziehen. Also, etwa alle Prozessoren der Hardware-Plattform zu erfassen, um der dynamischen Zuteilung von Ressourcen in virtuellen Umgebungen gerecht zu werden. Einige Software Hersteller unterscheiden bei der Lizenzierung zwischen den eigenen Virtualisierungs-oder Cloud-Technologien und denen anderer Hersteller. Oder sie machen die Lizensierung von Messgeräten abhängig, die sie zuvor zertifiziert haben. Kunden sollten ihre Lizenzverträge daraufhin prüfen und Kontakt zu ihrem Software-Hersteller aufnehmen und klären, welche Regeln in ihrem Fall zutreffen.

Die neuen Realitäten der Virtualisierung ermöglichen asynchrone Strukturen, die mehrere Hard- und Software-Elemente verknüpfen. Sie komplizieren SAM zusätzlich: So verbindet in einem typischen Anwendungsbeispiel eine Virtualisierungs-Ebene mehrere Hardwarekompo-nenten auf der einen und mehrere virtuelle Rechner (Betriebs-systeme) auf der anderen Seite. So ist es unmöglich, einen einzelnen Rechner einer bestimmten Hardware zuzuordnen.

Virtualisierung kann Organisationen viele Vorteile bringen - etwa niedrigere IT-Kosten, weniger CO2-Ausstoß durch gesenkten Energieverbrauch, bessere Business Continuity sowie flexiblere und schnellere Markteinführungen. Doch vor dem Hintergrund der Lizenzfragen ist Virtualisierung nicht kosteneffizient, solange sie nicht gut vorbereitet und umgesetzt wird.

Virtualisierung stellt SAM vor allem wegen der Messung und Verwaltung vor Herausforderungen. Virtuelle Maschinen können mit ein paar wenigen Mausklicks erstellt und gelöscht werden, ihre Konfiguration ändert sich oft und automatisch. Nicht selten werden virtuelle Maschinen aufgabenbezogen eingerichtet, wenn etwa einzelne Abteilungen arbeitstechnisch besonders stark ausgelastet sind oder Gruppen Tests und Entwicklungsprojekte starten. Später werden sie wieder gelöscht, ohne dass SAM-Prozesse durchlaufen werden oder die nötigen zusätzlichen Lizenzen für die verwendete Software gekauft wurden. Die große Dynamik der Virtualisierung zusammen mit der Unsicherheit der zutreffenden Lizenz-Reglungen gerade für Lizenzverträge, die schon lange bestehen, machen die Virtualisierung zu einem der schwierigsten SAM-Themen.

Software-Hersteller reagieren darauf auf verschiedene Weise. Ein Ansatz ist die Abkehr von Hardware-basierter Lizenzierung hin zu Anwender-basierten Modellen, Nutzungs-basierten Modellen (etwa der Zahl der Rechenoperationen) oder Ergebnis-basierten Modellen (zum Beispiel dem erzielten Umsatz). Eine andere Strategie ist es, dem Kunden spezielle Werkzeuge zur Verfügung zu stellen, um Hardware-Messungen in virtuellen Umgebungen vorzunehmen (so etwa das „IBM License Metrics Tool“, ILMT). Mit diesen Modellen können Organisationen ihr SAM in virtuellen Umgebungen im Sinne dieser Software-Hersteller effektiver lösen. Sie sollten sich aber nicht darauf verlassen, dass die Hersteller alle oder den Großteil der SAM-Herausforderungen der Virtualisierung für sie lösen.

Für den Endkunden beeinflusst die Virtualisierung das SAM erheblich. SAM-Programme müssen alle virtualisierten Elemente umfassen und die vollständigen Informationen zu den Software-Lizenzen haben, die von der Virtualisierung betroffen sind. SAM-Programme müssen gemäß der Entwicklung der Lizenzregeln der Software-Hersteller regelmäßig angepasst werden. Das erfordert besondere Sorgfalt, damit Virtualisierungs-Projekte keine negativen finanziellen Folgen haben. Zudem muss durch ständige Kontrollen der IT-Infrastruktur sicher gestellt werden, dass keine ungenehmigten Virtualisierungs-Technologien außerhalb des bestehenden Verwaltungsrahmens eingesetzt werden.

Eine Virtualisierungs-eigene Herausforderung des SAM ist die Disziplin beim Abbau von Beständen. Virtuelle Maschinen sind vom IT-Admin einfach und schnell zu erstellen , etwa um kurzfristigen Bedarf für ein Projekt zu decken. Oft wird vergessen, dass nach Abschluss des Projektes diese virtuellen Arbeitsplätze wieder zu löschen. Andernfalls sind die die zusätzlichen Lizenzen hier grundlos gebunden. In vielen Organisationen gibt es zahlreiche verwaiste virtuelle Maschinen. Keiner weiß, zu welchem Zweck sie ursprünglich geschaffen wurden. SAM-Programme sollten Kontrollen enthalten, die die zeitnahe Löschung ungenützter virtueller Maschinen sicher stellen.

Die Software-Hersteller haben Ratgeber und Regelwerke in verschiedener Detailtiefe entwickelt. In SAM-Programmen kann die Rolle der Virtualisierung nun nicht mehr einfach geschätzt werden, selbst wenn die bestehenden Lizenzverträge keine Aussagen dazu enthalten. Auch wenn die neuen Reglungen der Hersteller bei den Organisationen nicht immer auf Begeisterung stoßen, ist ein klares Verständnis für die Virtualisierungsregeln für ein erfolgreiches SAM-Programm unabdingbar.

Zusätzlich kompliziert wird SAM durch die Realität der gemischten Berechnungsgrundlagen, die in virtualisierten Umgebungen vorliegt. Organisationen haben ihre Software in den meisten Fällen teils vor, teils nach Aufkommen der Virtualisierung erworben. Dies führt verschiedene Lizenztypen für die gleiche Software mit sich. Diese werden die von der Virtualisierung auf verschiedene Art und Weise betroffen. Organisationen müssen mit den Herstellern zusammen arbeiten, um ihre Vorgaben zur Lizenzierung in virtuellen Umgebunden umzusetzen. Sonst drohen nach einem Audit unerwartete Kosten.

# SAM und Infrastructure/Platform as a Service

## In anderen Cloud-Modellen als dem SaaS (etwa IaaS/PaaS) stellt der CSP einen Teil der Software bereit, ein anderer kommt vom Kunden. Beispiele für IaaS/PaaS sind Amazon EC2, Microsoft Azure und IBM SmartCloud.

Im Falle von Software, die wie beim SaaS ***durch einen CSP bereit gestellt wird*** (also etwa Betriebssystem oder Middleware), sollte der Kunde sich bescheinigen lassen, dass der CSP voll lizenziert ist, die Software zu diesem Zweck zu verwenden. Für jede nicht selbst erstellte Software, die er seinen Kunden bereitstellt (was meist der Fall sein dürfte), benötigt der CSP eine Lizenz des Herstellers, die üblicherweise Teil einer Vereinbarung für Service Provider ist. Sie erlaubt dem CSP, die Software als Dienst für Dritte einzusetzen. Kunden sollten darauf bestehen, dass ihnen der CSP eine verbindliche Bescheinigung dieses Rechts vorlegt. Zudem sollten sie als Teil ihres Cloud-Vertrags Klauseln festlegen, die sie von der Haftung für etwaige Ansprüche Dritter wegen Urheberrechtsverletzungen des Dienstes freistellen.

Ein weiteres Risiko bei der Nutzung von Software eines CSP ist die Möglichkeit, dass es sich nicht um Originalsoftware handeln könnte. Wenn der CSP Fälschungen verwendet, ist es möglich, dass der Code unautorisiert geändert wurde (etwa durch die Einbettung von Trojanern), und so ein Sicherheitsrisiko für die Daten der Organisation darstellt. Weil der Kunde nicht weiß, welche Software der CSP verwendet, muss er sich auf anderem Weg von der Echtheit der Software überzeugen. Es empfiehlt sich, von Anfang an einen zertifizierten und vertrauenswürdigen CSP zu wählen und entsprechende Klauseln in den Vertrag aufzunehmen.

Im Falle von Software, die ***der Kunde selber bereitstellt,*** sollte er bedenken, dass zwei getrennte Verträge zu verwalten und einzuhalten sind: der mit dem Softwarehersteller und der mit dem CSP. Diese Tatsache kann das SAM in der Cloud vor folgende Herausforderungen stellen:

- *Lizenzübertrag in die Cloud.* Gegebenenfalls machen die Lizenzbedingungen die Übertragung von Softwarelizenzen in die Cloud von der Zustimmung des Software-Herstellers abhängig. So schließen einige Lizenzverträge den Einsatz außerhalb des Standorts oder der kunden-

Der folgende Auszug aus einer Lizenzvereinbarung ist ein Beispiel für eine Regelung, die verhindert, dass Software für den internen Gebrauch Dritten zugänglich gemacht wird (und die einen CSP ohne korrekte Lizenzen betreffen könnten): „Der Lizenznehmer hat nicht das Recht, Dritten die Software zu verleihen oder zu vermieten, als Softwarebüro oder im Zeitanteilsverfahren, als Application Services Dienstleister, als Hoster oder im Rahmen anderer Dienstleistungen anzubieten noch ihre Funktionen Dritten bereit zu stellen."

In manchen Fällen ist der CSP gleichzeitig ein Softwarehersteller, der die gleiche Software in zwei Kanälen zur Verfügung stellt: traditionell/physisch und in der Cloud.

eigenen Hardware grundsätzlich aus. Einige große Hersteller untersagen den Einsatz in der Cloud generell, andere machen eigene Cloud-Angebote, die das genaue Nutzungsvolumen der Software erfassen und zertifizieren einige CSP (aber nicht alle) für den Einsatz ihrer Software. Viele Software-Hersteller haben aber keine eindeutigen Richtlinien. Jeder ungenehmigte Übertrag von Softwarelizenzen in die Cloud kann für eine Organisation und eventuell auch für den CSP Schadensersatzforderungen zur Folge haben.

- *Unautorisierter Einsatz.* Eine Lizenz kann Beschränkungen enthalten, die die Übertragung von Lizenzen in die Cloud verbieten. Beispiele dafür sind:
  - Räumliche Einschränkungen — sie können ausgesprochen problematisch sein, da Kunden mancher Cloud-Dienste die Serverstandorte nicht kennen, nicht einmal die Länder;
  - Einschränkungen der Rechtsform, die von einer Lizenz abgedeckt wird — diese könnten den Cloud-Einsatz gegebenenfalls ausschließen;
  - Einschränkungen von Geräten oder Plattformen — sie könnten die Verwendung mancher Cloud-Umgebungen ausschließen und sind in der Verwaltung sehr anspruchsvoll, weil der Kunde von einigen Cloud-Systemen die technischen Spezifikationen der Architektur nicht kennt.
- *Messung von Hardware-bezogenen Metriken in der Cloud.* Die korrekte, vollständige und nachvollziehbare Messung von Hardware-bezogenen Metriken in der Cloud ist eine erhebliche Herausforderung für SAM, selbst wenn die Hardware in einer traditionellen Installation im kundeneigenen Rechenzentrum steht. Wenn hierzu IaaS/PaaS-spezifische Komplikationen kommen, wird die Aufgabe noch anspruchsvoller. Es könnte schwer fallen, Software, die der CSP besitzt oder bereitstellt, von jener zu unterscheiden, die vom Kunden kommt. Entsprechend könnten zu hohe oder zu niedrige Lizenzgebühren berechnet werden.
- *Audits durch den Software-Hersteller.* Die meisten Lizenzverträge enthalten Klauseln zu Audits, mit denen der Software-Hersteller nach Ankündigung zum Zwecke der Prüfung der Lizenztreue Zugriff auf und Zugang zu den Rechnern des Kunden erhält. Es ist unwahrscheinlich, dass dies vom Kunden im Rahmen einer Vereinbarung mit einem CSP gewährleistet werden kann. Selbst wenn es dem Kunden möglich wäre zu erfahren, wo in der Cloud die von ihm genutzten Server physisch stehen, wird er dem CSP diesen Zugang kaum abverlangen können. Damit handelt der Kunde potentiell nicht gemäß seiner Lizenzvereinbarung mit dem Software-Hersteller. In manchen Fällen wird es dem Kunden möglich sein, den Prüfern Fernzugriff auf die virtuellen Rechner in der Cloud zu geben. Dies könnte aber unzureichend sein, um die vollen Kennzahlen der zugrundeliegenden Hardware zur Lizenzberechnung zu ermitteln. Wenn man bedenkt, dass sich der Kunde die Hardware vermutlich mit anderen Kunden des CSP teilt, wird ihm der CSP keinen Zugriff darauf gestatten. Wenn zudem die Lizenzverträge Fristen für die Bereitstellung der Messdaten setzen, muss ein SAM-Programm mit dem CSP zusammenarbeiten, um diese Fristen einzuhalten.
- *Rückübertragung von Lizenzen aus der Cloud.* Das Unternehmen sollte ermitteln, ob es laut seines Cloud-Service-Vertrages, seiner Software-Lizenzbedingungen und der Richtlinien des Software-Herstellers nach Ende der Cloud-Nutzung seine Lizenzen wieder zurück übertragen kann. Dies mag in einigen Fällen die Zustimmung des Software-Herstellers und/oder des CSP voraussetzen.

# Über BSA | The Software Alliance

BSA | The Software Alliance ist die globale Stimme der Software-Industrie. In der BSA sind weltweit führende Unternehmen zusammen geschlossen, die jährlich Milliardenbeträge in neue Softwarelösungen investieren, welche die Wirtschaft antreiben und das moderne Leben von heute prägen.

BSA ist die führende Antipiraterie-Organisation und ein geschätzter Partner, wenn es darum geht, die technologische Innovation und das Wirtschaftswachstum zu fördern.

Durch internationale Zusammenarbeit mit Regierungen, die Verfolgung von Urheberrechtsverletzungen und breite Aufklärungsmaßnahmen arbeitet die BSA daran mit, den Horizont der digitalen Welt zu erweitern und das Vertrauen in neue Technologien zu stärken.

BSA ist die führende Antipiraterie-Organisation und ein geschätzter Partner, wenn es darum geht, die technologische Innovation und das Wirtschaftswachstum zu fördern.

## Schutz des Urheberrechts und von Innovationen

Das Recht am geistigen Eigentum – Urheberrecht, Patente und Markenrechte – ist die Grundlage kreativer Unternehmen und die Basis wirtschaftlichen Wachstums. Diese Rechte sind auch für die kommerzielle Entwicklung von Software von zentraler Bedeutung. Software-Entwicklung ist im Hinblick auf Urheberrechte die weltweit größte Branche.

Gemeinsam mit politischen Entscheidungsträgern, durch Rechts- und Aufklärungsinitiativen rund um die Welt trägt die BSA dazu bei, dass das Recht am geistigen Eigentum in der Weltwirtschaft und der Gesellschaft geachtet wird.

- **Schutz des geistigen Eigentums:** Die BSA unterstützt Regierungen weltweit, um zu gewährleisten, dass der Schutz des geistigen Eigentums mit den neuen Technologien wie Cloud Computing Schritt hält.
- **Einschränkung des Softwarediebstahls:** Die BSA hilft ihren Mitgliedern weltweit durch aktive Rechtsprogramme beim Kampf gegen Software-Diebstahl, indem Lizenzvergehen von kommerzieller Seite oder Endnutzern, Fälschung und Internetpiraterie rechtlich verfolgt werden.

- **Marktforschung:** Die BSA ist Autor der wichtigsten Studien über Piraterie und ihrer wirtschaftlichen Auswirkungen weltweit. Sie beleuchtet die Ausmaße des Problems und hilft dabei, nationale und internationale politische Strategien zu entwickeln.
- **Aufklärung:** Die BSA klärt Verbraucher über die negativen Folgen der Softwarepiraterie auf und bietet Tools und Trainings an, um Organisationen dabei zu unterstützen, ihren Softwarebestand effektiv zu verwalten.

## Öffnung neuer Märkte und Schutz des freien Wettbewerbs

- Der freie Marktzugang ist für wirtschaftliches Wachstum und Wohlstand entscheidend. Die BSA eröffnet der Softwareindustrie Marktchancen, indem sie Regierungen dabei unterstützt, Handelsschranken aufzuheben und Benachteiligungen bei öffentlichen Ausschreibungen zu verhindern, die wettbewerbsverzerrend sind und Innovation behindern.
- **Abbau von Handelsschranken:** Die BSA informiert Entscheidungsträger durch Expertenmeinungen und Marktanalysen, um eine Strategie offener Märkte zu fördern. Sie legt dabei ihren Fokus auf die BRIC-Staaten, die zu den am schnellsten wachsenden Technologiemärkten zählen, in denen die Piraterie jedoch weit verbreitet ist.
- **Förderung von technologischer Neutralität:** Die BSA unterstützt international anerkannte Standards und unvoreingenommene Ausschreibungsverfahren für IT-Projekte, um den fairen Wettbewerb zu ermöglichen.
- **Förderung der Innovation:** Die BSA arbeitet mit politischen Entscheidungsträgern weltweit zusammen, um ein Umfeld zu schaffen, in dem neue Technologien wie Cloud Computing gedeihen. Neben der Zusammenarbeit bei technologischen Standards umfasst dies den verbesserten Schutz für geistiges Eigentum, die Harmonisierung internationalen Rechts und die Behandlungen derjenigen Herausforderungen, die nicht durch ein einzelnes Unternehmen oder eine einzelne Regierung zu lösen sind.

## Vertrauen in neue Technologien

Sicherheit und Datenschutz sind Grundsteine des Vertrauens in die Informationstechnologie für Verbraucher, Unternehmen und Regierungen. Die BSA unterstützt den verantwortungsvollen Umgang mit Daten und die Akzeptanz von Innovationen, die den Technologiemarkt verändern und der ganzen Gesellschaft nützen.

- **Förderung von öffentlicher und privatwirtschaftlicher Zusammenarbeit:** Auf Basis des Fachwissens ihrer Mitglieder und der produktiven Zusammenarbeit mit Beamten und Amtsträgern versteht sich die BSA als Wissensvermittler und Unterstützer der Zusammenarbeit und Konsensbildung zwischen Industrie und Regierungen.
- **Verbraucherschutz:** Angepasst an neue Technologien wie etwa Cloud Computing entwickeln die BSA und ihre Mitglieder angemessene Standards zum Schutz der Privatsphäre und der Sicherheit und teilen diese Erkenntnisse mit Politik und Verwaltung.
- **Politische Lösungsfindung:** Die BSA hat einen globalen Rahmen für Cyber-Sicherheit entwickelt, um Regierungen bei der Entstehung von Gesetzen zu unterstützen, die Cybercrime ahnden, Bedrohungen vermeiden, Verbraucher informieren und schützen sowie die Reaktion auf Cyber-Angriffe ermöglichen.

**Quellen**


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


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

Niederlassung
Deutschland
Wilhelmstraße 21
80801 München

T: +49.89.321.519.87

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 Vietna