Deloitte.

Flashpoint

Software asset management (SAM)

Getting smart about a new engine for IT business value

Making sense of your enterprise software

As top information technology (IT) leaders continue to feel the pressure to unlock value for the business, some have turned their attention to one of their biggest IT budget items: software. For many companies, software licensing and maintenance activities consume close to 22 percent of the IT budget[1]—thanks to the ever-expanding role of software.

In an era marked by increasing amounts of digital data, an emphasis on process automation, and the importance of apps, software has become an enabler of efficiencies. But given the massive role that software now plays in the enterprise, software itself has become a prime target for efficiency efforts. Many enterprises lack a clear view of their software asset picture—failing to know the quantities of licenses they own and failing to understand the actual extent to which they have deployed software. That incomplete view can lead to underutilisation as well as overutilisation of software licenses.

To begin bringing the software picture into better focus, CIOs are turning to software asset management (SAM) practices—coordinated, comprehensive programmes and policies that seek to control software expenditure, capitalise on volume discounts, avoid non-compliance with licensing contracts, and deploy software more efficiently. Many organisations are underpinning these SAM practices with intelligent discovery and inventory SAM tools to further enhance efficiencies.

It's an approach that can help avoid costs and align spending with consumption—which can free up financial resources that can be reinvested in business activities and help make a SAM programme self-funding. Such savings can be significant. For example, in software license assessments performed by Deloitte, clients had unrealised cost savings averaging 23 percent of their annual maintenance spend.[2] The SAM approach can also help improve the budgeting process, boost financial controls, curb cyber risk, and help reduce audit concerns.

An effective SAM approach requires more than updating your catalog of software and formalising processes. Organisations that intend to leverage SAM as a driver of value and performance should understand that managing software assets in today's fast-changing IT environment requires a deep understanding of the issues. Here's a look at a few key issues emerging with SAM.

About *Flashpoints*

Every day brings new ideas and possibilities to the Technology, Media, and Telecommunications sectors. *Flashpoints* is your tool for gaining the context you need to make sense of these critical developments—as they emerge.

1. IT Metrics: IT Key Metrics Data. Gartner, Inc. December 14, 2015
2. Deloitte Advisory results and analytics related to cost savings/avoidance come from a dataset composed of roughly one thousand software license assessments performed across 20 countries between 2015 and 2018. Included data was normalized, removing outliers and calculating values at contracted prices

Key observations

Convergence with IT asset/ service management

The discipline of SAM is rapidly converging with IT asset and service management disciplines, offering a more comprehensive view of activities as well as new capabilities for IT leaders.

An opportunity to tighten cyber security

Without an effective SAM programme, some software can remain hidden from the view of IT leaders—meaning that the organisation might not be patching, updating, or securing it properly to reduce the risk of a cyber intrusion.

When others manage the infrastructure: moving licenses to the cloud, outsourcing data centers

Despite the simplicity promised, cloud activities and data center outsourcing can present complex challenges for SAM. Missed steps could result in your organisation operating in an unlicensed environment.

Software as a service: subscription model considerations

A subscription model can offer hassle-free access to software while reducing licensing risks. But you might be overpaying and getting more than what you really need, failing to consider the full costs and benefits.

Convergence with IT asset/service management

As organisations continue to emphasize managing IT like a business, efforts are intensifying around IT asset management and IT service management. Within organisations today, new sets of policies and procedures are emerging to give leaders guidance on how to ensure IT operations run efficiently. The discipline of SAM is rapidly converging with IT asset and service management disciplines—in part because new automation tools make it easier for businesses to integrate efforts and see across IT activities.

The result is that changes to the IT environment are no longer looked at just from the standpoint of security or operational efficiency. Increasingly, changes to the environment are viewed also through the lens of vendors and licenses. The trend is especially obvious when it comes to patch management, which touches on the traditional security aspect of IT management while heavily involving licensing and related concerns that come with putting in place new or updated software.

On a deeper level, what the convergence means is that workers increasingly will have the ability to manage SAM needs within the same platform they use for traditional IT asset/service management. And that convergence helps support new possibilities for managed services or centralisation of efforts—freeing some organisations from the burden of having to be SAM or IT management experts, helping them to gain a more comprehensive picture of software assets, to optimise software activities, and to reduce or avoid related costs. Such new comprehensive capabilities can be especially helpful when the organisation is trying to align software asset status with ever-changing product names and license-counting methodologies from vendors, or when the security team needs to rapidly pinpoint which applications have been patched.

Ultimately, the convergence and related functionality mean that organisations can support integrated governance around software assets, boost their compliance, and help reduce the risk of audit.

The discipline of SAM is rapidly converging with IT asset and service management disciplines, offering a more comprehensive view of activities as well as new capabilities for IT leaders.

An opportunity to tighten cyber security

Not knowing what you have is a risk. And where there is software, there is the potential for security breaches. But given today's chaotic enterprise software landscape, CIOs sometimes don't know what they have. For example, it's not unheard of for the CIO to be completely unaware of the existence of an entire data center within his or her organisation.

Such "hidden" operations can represent significant instances of software that are effectively off the radar of leadership—and potentially not being patched, updated, or secured properly to reduce the risk of a cyber intrusion.

Consider developing a complete catalog of software that has been approved from a functionality perspective as well as a security perspective. A SAM approach can allow you to inventory assets so that you can then ensure that they are secured.[3] Getting started involves a data inquiry as well as a "corroborative" inquiry within your organisation. Where do you have data and where is it even possible to have software running? How complete is your view of the hardware on which software runs? What will it take to develop a comprehensive, content-rich, data-rich portfolio that multiple teams or functions within the organisation can leverage? Determining thoroughly where all your software assets lie allows you to define your cyber perimeter and then fortify and defend it through regular patch management activities and proactive monitoring, for example. Also consider developing a formal request process so your IT organisation can vet software that business units might wish to acquire.

The "SAM and security" approach also requires you to look closely at your virtual data centers, too—to know the number of virtual machines and software stacks in play and to place security protocols right on top of a virtual machine each time a new one is created.

As the virtualisation trend continues, your organisation might continue to undertake major digital transformation efforts, all while complying with changing regulatory requirements around data practices. Consequently, your software and software vendor landscape can become even more complex, requiring you to focus continuously on defining and securing the "fence" around your software assets as well as investing in your cyber risk framework.

Without an effective SAM programme, some software can remain hidden from the view of IT leaders—meaning that the organisation might not be patching, updating, or securing it properly to reduce the risk of a cyber intrusion.

3. Minimizing the threat landscape through integration of Software Asset Management and Security. Deloitte. 2015. http://www2.deloitte.com/us/en/pages/risk/articles/software-asset-management-security-report.html.

When others manage the infrastructure: moving licenses to the cloud, outsourcing data centers

Moving business functions to the cloud offers many organisations an opportunity to simplify their operations. Why develop IT infrastructure and platforms in house when a cloud provider can do the work for you while also overseeing maintenance and upgrade needs? Despite that simple premise, cloud presents some complex challenges when it comes to SAM. What you don't know can lead to missed steps and possibly result in your organisation operating in an unlicensed environment.

If the idea of working with a cloud provider to get infrastructure/platform-as-a-service capabilities and essentially "migrate" your existing software applications to the cloud appeals to you, you should recognise that a bring your own licenses (BYOL) approach requires a deep understanding of what your software licenses actually entail. In BYOL models, companies can choose to "certify" that they already have end-user licenses that can be hosted in the cloud. In such a scenario, companies can create their virtual solutions in the cloud in the same manner they would in a software as a service (SaaS) model. In this example, both the third-party hosting (cloud) provider and the company take on licensing risk.

Many software vendors have included in their contracts restrictions that address whether a license can be used on premises or off premises. Moving to the cloud to address hardware infrastructure or platform needs doesn't mean that your licensing issues—such as the potential for violations and penalties—go away. Restrictions remain the same and in many cases issues can become more complex if, for example, a cloud provider instantly scales up infrastructure from, say, eight servers to 16 servers to meet growing demand from your software user base. Having a cloud-readiness strategy that addresses SAM complexities is essential.

Likewise, when it comes to the outsourcing of data centers, realise that service providers are more focused on service level agreements—on keeping hardware up and running to meet your needs—than they are on tracking license issues that might emerge when they make hardware changes. Ultimately, as you work with cloud or data center providers, SAM issues will be yours to oversee and manage.

Despite the simplicity promised, cloud activities and data center outsourcing can present complex challenges for SAM. Missed steps could result in your organisation operating in an unlicensed environment.

Software as a service: subscription model considerations

In addition to bringing their own software licenses to the cloud, many organisations are choosing to purchase cloud-based SaaS. Businesses and consumers alike, in fact, are showing a preference for SaaS subscription models when it comes to the provision of some services and content. A subscription model can offer you full access to a service or a tier of services in a way that removes some risk from the picture. For example, you no longer need to worry about constantly evaluating your usage needs and right-sizing your purchase of services. And when it comes to software in particular, you can reduce audit risk and the risk of operating in an unlicensed environment because you no longer need to fuss with self-policing your organisation's software copies, usage, and license restrictions, since the relevant controls are embedded into the subscription model by the software provider.

But the reality is that in reducing some risks and gaining potentially unfettered "full access" to software offerings, the new risk you face is in paying for more than what you are using. In a SaaS model, some hosting companies often charge their customers by usage metrics—for example, named-user access to certain feature sets within a product, or a price per hosted solution. So know what you are really using. What do you really need? Are you paying for the subscription model that most closely fits your business and IT needs? SAM practices for your organisation should take into consideration the full costs and benefits of subscription-based software.

For many organisations today, however, subscription services constitute a small portion of total IT spend—many major players are still selling under a perpetual license model. But as new digital capabilities evolve across the business spectrum, as new software players emerge, and as vendors see new market opportunities for subscription models, the subscription trend will likely grow. Your SAM approach should be prepared to address subscription-model-related issues that arise. And for some organisations, working to develop a flexible consumption business model for software needs—consistent with a "pay for what you actually use" utility model—may make more sense for the business.

A subscription model can offer hassle-free access to software while reducing licensing risks. But you might be overpaying and getting more than what you really need, failing to consider the full costs and benefits.

Let’s talk

The potential of SAM represents a new path to value for IT leaders, but understanding the complexities involved in launching or expanding a SAM programme requires careful review of key issues. Outsourcing needs, management trends, security concerns, and new business models are just part of the picture. SAM issues extend to your core business processes, workforce considerations, regulatory concerns, and more.

For large organisations, especially, the complexities of managing software assets and licenses represent challenges that might be better shifted to third parties specialising in SAM issues. Understanding the SAM options and putting together all of the pieces into an effective and cohesive strategy requires a conversation. Want to know what a strong SAM managed services programme looks like? We should talk.

Contacts

Southern Africa

Navin Sing
Managing Director:
Risk Advisory Africa
+27 83 304 4225
navising@deloitte.co.za

Sisa Ntlango
Risk Advisory Africa Leader:
Internal Controls & Assurance
+27 82 920 3677
sntlango@deloitte.co.za

Nombulelo Kambule
Associate Director:
Risk Advisory Southern Africa
+27 82 549 8603
nkambule@deloitte.co.za

Central Africa

Tricha Simon
Risk Advisory Regional Leader:
Central Africa
Mobile: +263 772 234 932
Email: tsimon@deloitte.co.zm

Rodney Dean
Director: Risk Advisory
Central Africa
Mobile: +263 772 263 016
Email: rdean@deloitte.co.zm

East Africa

Julie Akinyi Nyangaya
Risk Advisory Regional Leader:
East Africa
Mobile: +254 72 011 1888
Email: jnyangaya@deloitte.co.ke

Urvi Patel
Director: Risk Advisory
East Africa
Mobile: +254 71 158 4007
Email: ubpatel@deloitte.co.ke

West Africa

Anthony Olukoju
Risk Advisory Regional Leader:
West Africa
Mobile: +234 805 209 0501
Email: aolukoju@deloitte.com.ng

Temitope Aladenusi
Director: Risk Advisory
West Africa
Mobile: +234 805 901 6630
Email: taladenusi@deloitte.com.ng

Deloitte.