Real experts.
Real data.
Real savings.

SmartSpend™ Bulletin

How the Cloud is Changing Everything We Know About Software Audits

For on-premise IT, vendors have been the "auditors" – policing customers to assure license compliance. In the cloud, vendor audits are no longer a necessity. Customers are free to consume (and spend) all they want, and are in a constant state of compliance because vendors are directly authorizing access rights. Responsibility – and the purpose – for audits have shifted 180 degrees. Without regular self-audits of cloud usage and without detailed usage data from vendors, many companies may find themselves overbuying and overspending.

For enterprise IT and sourcing professionals, the topic of software license audits is a hot button. Discourse and frustration are primarily focused on two points:

1. IT vendors are conducting more licensing audits as they transition from on-premise to cloud offerings.
2. Noncompliance penalty fees are becoming stiffer.

Enterprises have growing concern and frustration. It's not uncommon for a company to undergo large-scale licensing audits from multiple vendors in the same year. Furthermore, a vendor's audit findings are usually incorrect, and defending against them is costly and disruptive. At the end of the day, a true compliance position is usually achieved, but it's a painful process.

But what about audit risks in the cloud? Do they even exist? What are they? How are they different from the risks associated with traditional on-premise audits? The answers to these questions may surprise you.

THE CLOUD HAS REDEFINED AUDIT RISK – HERE'S WHAT YOU NEED TO KNOW

To understand how the cloud has impacted everything we know about audits, let's first view audit risk and responsibility from an IT vendor's perspective in an on-premise setting. Improper or under-licensing across a vendor's customer base is a credible and significant threat to revenues. That threat has grown as customers' IT ecosystems have evolved to become more tightly integrated and include more devices and users, and as IT spending and asset management have become more decentralized. Of course, every enterprise wants to abide by their licensing rights and obligations, and it is extremely rare to find intentional non-compliance. But vendors know that unintentional non-compliance is common – especially when licensing rights are (in most cases, intentionally) complex.

In the cloud, the risk and responsibility model for audits gets turned on its head. **What was once the role of the vendor is now the role of the customer**.

Without audits, vendors have little visibility into the state of licensing compliance with a particular customer. While some vendors have taken a more predatory stance on licensing audits in the past year (mainly as a way to "motivate" customers to migrate to newer cloud offerings), vendors do have a right to enforce their licensing policies and to collect appropriate fees when customers are improperly licensed.

In the cloud, the risk and responsibility model gets turned on its head. For the most part, vendors have deep visibility into cloud usage and compliance. The risk of under-subscription is minimal because the vendor is directly authorizing usage rights. If a customer needs a seat/subscription, they pay the fee or they don't access the vendor's solution. There is no reason for vendors to conduct audits.

In a cloud scenario, *lack of visibility into usage has shifted from the vendor to the customer.* Therefore, the audit responsibility doesn't lie with the vendor – it lies with the customer. In order to avoid overbuying and overspending, enterprises have to regularly audit usage to determine if spend and usage are aligned. There is certainly no risk for the vendor if the company is oversubscribed.

The issue of visibility is key here. *Vendors are not motivated to provide their customers with detailed usage data and insights.* In fact, the usage data that most cloud vendors provide to their customers is a 10,000-ft. view articulated through slick dashboards. The lack of granular detail makes it difficult for customers to accurately analyze functionality usage, license type usage, which subscriptions are idle, seasonal/peak usage, etc.

FOUR RECOMMENDED ACTIONS TO TAKE

To avoid overspending and overbuying in the cloud, companies should self-audit cloud usage with key vendors and take the following steps:

- Perform usage analysis and subscription optimization. Understand your organization's unique usage profile. How many subscriptions are actually being used and how often? Are you paying for more "power user" subscriptions than you actually need? What about peak/seasonal usage? These are just a few of the questions that need to be asked in order to optimize subscriptions. Consider this: Recent research indicates less than 40 percent of the Microsoft Office 365 licenses/subscriptions that have been purchased are actually in use.

To avoid overspending and overbuying, enterprises need to **conduct regular self-audits of cloud usage** with key vendors.

- Take advantage of subscription flexibility. Unlike on-premise licensing, cloud subscriptions are more cut-and-dried. But that doesn't mean some vendors won't be flexible in their offerings. Depending on your usage profile, consider asking for "restrictive use" or other unconventional subscription types that better suit your organization's usage.
- Benchmark pricing and use vendor-specific intel to inform negotiations. Cloud pricing and discounts are becoming more variable, making it difficult for customers to determine if they're paying a best-in-class price. Vendor flexibility at the negotiation table is evolving quickly as they reconcile changes in business strategy with investor and shareholder expectations. NPI advises enterprises to benchmark pricing, discounts and terms as well as bring vendor-specific negotiation intel to every deal.
- Set a regular cadence for internal usage audits for key cloud vendors. Depending on the significance of the spend, how often you are adding seats/licenses and the timing of renewal dates, establish a formal, scheduled self-audit action item for your top cloud implementations. For example, a typical large Salesforce.com account renews annually, and there may be a significant number of additions throughout the year as team members come and go. Meanwhile, other users are idle or their roles change, and their seats could easily be repurposed or downgraded. Conduct a self-audit at month 5 and at month 10 so you're completely on top of usage optimization and prepared for the renewal in terms of requirements.

ABOUT NPI

NPI is an IT sourcing consulting company that helps enterprises identify and eliminate overspending on IT purchases, accelerate purchasing cycles and align internal buying teams. We deliver transaction-level price benchmark analysis, license and service optimization advice, and vendor-specific negotiation intel that enables IT buying teams to drive measurable savings. NPI analyzes billions of dollars in spend each year for clients spanning all industries that invest heavily in IT. For more information, visit www.npifinancial.com.

NPI Headquarters
271 17th Street
Suite 550
Atlanta, GA 30363

T 404-591-7500
F 404-591-7501
E info@npifinancial.com

NPI Real experts. Real data. Real savings.