Hewlett Packard Enterprise

Business white paper

Avoiding audits

How to get off software vendors' radar

Table of contents

The software audit police

Leisurely driving down the highway, you pass a police car parked behind some bushes. After the officer pulls you over, he asks, "Do you know why I pulled you over?" Your honest response might be, "No, officer … I wasn't really paying attention."

Much like their civil counterparts, those who enforce software license compliance are drawn to indicators that suggest potential wrongdoing. Although there are some vendors that check compliance among their customers on a random basis, the vast majority of software vendors are selective about whom they choose to audit. The main consideration is the **expected return of the audit**.

Make no mistake! Vendors certainly have a legitimate interest and legal right to guard their intellectual assets against abuse. Audits consistently show that only a minority of organizations are able to demonstrate they are abiding fully by the terms of their licensing agreements. While some software vendors may seek to take advantage of their customers' noncompliance to drive additional revenues, many are merely seeking compensation for the value their customers have obtained through their use of software.

Regardless of whether the objective is to receive fair or excessive compensation, each audit is a business endeavor with a cost of performing the audit, an expected return of settling noncompliance issues, and a risk that the actual benefits won't cover the incurred costs. Attention is certainly given to those opportunities that offer the highest return on investment with the lowest risk.

This paper will make you aware of many of the factors that signal potential noncompliance. It should also become apparent that the only surefire way to limit these factors and avoid audits entirely is by adopting a comprehensive approach to Software Asset Management (SAM). Besides minimizing the risk of audits, SAM will enable your organization to **make better business decisions, achieve cost-efficiencies, get more value out of its software investment**, and of course, **use its business assets ethically and professionally**.

Why—and why wouldn't—they audit you?

Before examining the telltale signs of compliance problems, it's important to understand why a vendor would audit a valued customer. Both qualitative and quantitative considerations will influence the decision to audit.

First and foremost, the relationship with the customer is at stake. Depending on how fairly the audit is conducted and a settlement arrived at, the relationship with the customer could suffer significant damage, which will invariably have consequences for future sales. But because many vendors' audit functions are organizationally separate to sales and thus driven by different metrics, it shouldn't be a surprise to find that vendors often sacrifice long-term relationships for the short-term gains obtained through audits.

A key consideration that may weigh on the minds of vendors that are genuinely interested in helping customers achieve compliance is whether the organization is actively trying to adopt better SAM practices. Since the same resources that would be required to respond to an audit would also be involved in leading the organization toward proactive license compliance, the vendor may likely perceive an audit as counterproductive at the time and elect to postpone it. On the other hand, less benevolent vendors that look to take advantage of customers' compliance issues may see a secondary benefit in keeping them in a state of noncompliance.

The quantitative audit costs for the vendor mainly include overhead associated with the permanent audit staff and the fees paid to third parties who may actually execute the audit. Depending on the terms of the agreement, the latter of these is often borne by the customer if significant noncompliance is found. In rare cases, customers have been able to include within their agreements clauses that make the vendor or auditor liable for costs associated with the disruption of business resulting from audit activities, which the vendor should also bear in mind.

A vendor's expected returns from an audit will be primarily financial and can include not only fines, but also the purchase of new licenses and backed maintenance—often both at list price rather than a customer's discounted rate. An audit, or even just the threat thereof, can also act as an incentive for a customer to adopt a new product or licensing instrument from the vendor. For example, one of the benefits of volume agreements is the simplification of license tracking. And, of course, audits can help vendors identify abuse of software that leads to lost revenue, even beyond the confines of the organization they're auditing.

In the end, when deciding to audit a customer, the vendor weighs the expected returns against the probable costs, both of which are dependent on the degree of noncompliance that they can prove. To gauge this, the vendor will look for signs that suggest a customer isn't managing license compliance with sufficient diligence.

The broken taillights of license compliance

Traffic police scan passing cars looking for signs that suggest wrong doing: red sports cars are obvious, but more subtle indicators could include a broken taillight, expired license plates, or even an unwashed exterior. So how does a vendor identify an attractive audit target? By observing both regular behavior patterns as well as being sensitive to ad hoc signs, the vendor can often get a good impression of the customer's current priorities and challenges that might lead to noncompliance.

Purchasing patterns

The most obvious data source vendors keep an eye on is license purchases. Not only will this allow a vendor to determine what entitlements the organization has, but also what it doesn't have. For example, the use of Microsoft® SharePoint requires not only SharePoint Client Access Licenses (CALs), but also underlying SQL CALs. Failure to purchase the underlying SQL CALs when buying SharePoint CALs will not only signal an immediate compliance issue, but it also indicates a lack of licensing knowledge that could lead to other issues. A host of irregular purchasing behavior can also arouse suspicion: failure to renew maintenance or support agreements, multiple entities in an organization ordering similar types of licenses, or the ownership of older product versions. Such behaviors suggest lack of process control and/or decentralized purchasing that complicate license compliance efforts.

Comparing data sets

While it can be revealing to examine license purchase information alone, considerable insight can be generated by reviewing it in the context of other information sources. For example, if the vendor's support center has been receiving calls for a product that the organization has few or no licenses for, this may suggest widespread unlicensed use. Or, regular product downloads from the vendor's site without an accompanying license purchase after a trial period expires can signal unlicensed use of trial software instances. Compliance issues may also be expected if the customer's level of purchasing deviates significantly from an expected profile, as established by comparing the organization's size and other characteristics with its industry peers. Some vendors also promote the use of tools whose stated purpose is to assist with incident and problem resolution, but whose data can also be compared to entitlement information for the purposes of gauging compliance.

Ad hoc observations

While the analysis of regularly updated data can help establish a pattern of software use and compliance, a telling picture emerges when corroborated with ad hoc observations or information. While the ethics of the practice is debatable, tips about software misuse from disgruntled employees seeking compensation is one source of information industry organizations and vendors benefit from in seeking to identify noncompliant organizations. And while the intent certainly isn't mischievous, the odd comment about using a development environment for production purposes or availing of premium functionality when the organization only has rights to standard features could prompt further investigation. Similarly, some vendors and auditors will stay attuned to indications that the organization is taking steps that tend to complicate compliance efforts. License compliance is unfortunately an often overlooked topic during mergers, acquisitions, divestitures, and even outsourcing but at the same time, media coverage of these events is readily accessible. If the organization is seeking advice or support for rolling out a new technology, but this isn't reflected in license purchases, vendors may pick up on the incongruity.

Key points

- The only way to effectively mitigate the risk of noncompliance is by adopting SAM.
- HPE can help your organization plan, launch, and maintain your SAM initiative. Contact us today to learn how we can help you achieve your SAM goals.

Past experience

Of course, past experience is a good indication of future behavior. Because systemic problems that lead to noncompliance are not easily corrected, failure to demonstrate compliance in one audit makes an organization a good candidate for future audits by the same or other vendors.

Finally, it should be noted that typically it isn't just one red flag that would lead to a vendor deciding to audit a customer rather a pattern of several factors that illustrate a general situation of noncompliance.

Getting off the vendor's radar

By now, you've probably realized that with the myriad of indicators that could suggest noncompliance and an organization's general inability to consistently control all of these, simply adopting cosmetic measures to become less conspicuous in the vendors' eyes isn't practical. The only way to effectively mitigate the risk of noncompliance is by adopting the comprehensive approach to managing license compliance that SAM prescribes. By stressing fundamental, transformative change, the organization builds compliance from the inside out and won't have to worry about hiding compliance problems, because they will already be addressed.

In conjunction with adopting better SAM practices, organizations can take other steps to reduce the likelihood of being audited. First, discuss with your vendors openly, but prudently, your SAM efforts and licensing. Show them that your organization understands and takes licensing seriously, and if appropriate, is investing in enhancing its capabilities to proactively maintain compliance. Conversely, make it clear that you expect your sales representative to provide you updates and assistance regarding any significant licensing changes.

Second, create an audit response process. Although this won't prevent an audit, it will help an organization to provide a professional early response that will filter out "compliance fishing" attempts, avoid missteps that could signal uncertainty or doubt, and could be instrumental in an early conclusion to the audit.

HPE is there to help

HPE is the ideal partner to help your organization become a less-attractive audit target. Drawing upon HPE's familiarity with vendor programs, leading technology and processes, and proven approaches, your organization can adopt better SAM practices faster, more effectively, and with less risk. From the tools you need for your own on-premise solution to a complete managed service; from an initial consultation to a guided adoption of SAM, HPE can tailor a solution to your needs.

To discuss how HPE can assist your organization with adopting better SAM practices that will not only make it possible for your organization to address compliance but will also reduce costs and optimize value derived from your software investment, contact us today.

Learn more at
hpe.com/software/itam

Sign up for updates

Hewlett Packard Enterprise

4AA5-1217ENW, March 2017, Rev. 1