# Software Audit Risks – What Are the Chances Your Company Will Be Next?

**By Christopher Barnett**

There is a set of related questions our software-audit clients frequently ask us that boil down to variations on one or more of the following: Why am I being audited? What if anything did I do to cause this? How can I avoid it in the future?

Unfortunately, those questions often do not have clear answers.

Most software publishers offer little, meaningful information regarding their criteria for initiating audits of their customers. Any publisher will initiate a review if it receives information indicating that software is being used without sufficient licenses rights. However, while that model may be standard for audits initiated by BSA | The Software Alliance ("BSA") or by the Software & Information Industry Association ("SIIA"), it likely is not the norm for the majority of publisher-initiated audits. Most publishers will tell you that their standard procedures result in all of their customers eventually being audited, and that, in effect, it is just a matter of time before your company's name is called. This probably is true to an extent, though it does not tell the whole story.

The mere fact that some publishers run different "flavors" of audits should clue everyone in to the fact that not all reviews are conceived from the same set of circumstances. Microsoft is probably the best example of this, in that it currently audits its customers through an array of processes, including:

- **Audits initiated by the BSA.** These reviews almost always are based on anonymous allegations of unlicensed use and typically entail penalties that must be paid to the BSA in order to obtain releases of liability. (Note: Microsoft is not currently a member of the SIIA's anti-"piracy" program.)

- **Software Asset Management ("SAM") engagements.** Under this model, Microsoft engages a third-party vendor to offer optional license-review services at no charge to the customer. (We typically advise our clients to decline such invitations.)

- **Certified self-audits.** Here, the customer completes an internal review of its license position, purchases licenses to address shortfalls discovered (if any) as a result of the review, and returns a signed certificate to Microsoft confirming the completion of the process. (Unlike SAM engagements, these are not optional reviews, though no deployment information is shared with Microsoft or its vendors.)

- **Verified self-audits.** In this alternative, the customer provides information regarding the Microsoft products deployed in its environment and then purchases any licenses determined by Microsoft to be required based on that information. (Again, not optional reviews, but the auditors typically do not try to independently validate the deployment information.)

- **Third-party audits.** These are the most common types of audits where our clients ask us for assistance. Here, Microsoft typically engages an accounting firm like KPMG, Deloitte & Touche, or PriceWaterhouse to run the audit process, to collect deployment data from the customer, to validate that data (often through an on-site meeting at the customer's location, though sometimes through a remote, web-based meeting), and to prepare a report of its findings. Microsoft then uses that report as a basis for its compliance demand.

- **Third-party on-site audits.** This is the audit equivalent of The Boogeyman, though it is more of a theoretical possibility than a practical risk for most licensees. Microsoft's agreements contemplate the possibility that it could initiate an audit to take place at the customer's location (rather than simply having an on-site validation meeting at that location). However, the very nature of such an audit in many cases would result in it "unreasonably interfering" with the licensee's business operations, in violation of Microsoft's audit rights. Moreover, the review would represent a level of intrusion that we likely would not advise most of our clients to accept. Nevertheless, it remains a threat that Microsoft could use to secure heightened cooperation within the scope of one of the other audit alternatives.

The very fact that Microsoft has so many ways to take a bite at the apple indicates that it likely has some methodology for prioritizing its customers for certain levels of "treatment." While we almost certainly never will learn all of the details associated with its triage procedures, there do seem to be certain license programs or relationship events that may precipitate receipt of a notice letter (and these generally are common to all software publishers):

- **SPLA.** All things being equal, businesses with Services Provider License Agreements with Microsoft probably face a higher likelihood of being audited – and a higher likelihood of that audit being a third-party audit – than businesses that only have "traditional" volume-licensing agreements with Microsoft. SPLA represents a recurring revenue source for Microsoft, and it also entails third parties (the SPLA licensee's customers) having access to Microsoft programs without those third parties having a direct, contractual relationship with Microsoft. Given that, Microsoft has a heightened interest in policing the program more heavily. New SPLA licensees should expect an audit at any time, though the risk seems to be a little higher either in the second or third year of the first SPLA renewal (SPLAs almost always have three-year terms) or sometime during the first renewal term following the first full renewal term following the last audit

  Companies with similar kinds of "commercial hosting" licenses with other publishers also should consider themselves to being at a heightened risk for audits.

- **Termination of License Agreements.** If you decide not to renew a recurring-renewal license agreement (like an Enterprise Agreement or a SPLA) or if you follow the process for terminating such an agreement early, then you should expect for your company to be audited, and you should prepare accordingly. Keep in mind that many publishers' audit rights typically extend after the end of a license agreement (and in some cases, indefinitely).

-

- **Failure to Satisfy Contractual Obligations.** If your company fails to do all the things it is supposed to do under its agreements, you also should expect to receive an audit notice letter. Failure to timely submit true-up orders or update statements under Microsoft's Enterprise Agreement enrollments is a prime example.

There also may be other risk factors specific to your company's relationship with its licensors. If you can see any of the above or other descriptions being applicable to your company, you need to take steps to ensure that you are doing everything you can to track your software asset usage and to ensure that you have acquired or reported all license rights to cover such usage.

**About the author Christopher Barnett:**

Christopher represents clients in a variety of business, intellectual property and IT-related contexts, with matters involving trademark registration and enforcement, software and licensing disputes and litigation, and mergers, divestments and service transactions. Christopher's practice includes substantial attention to concerns faced by media & technology companies and to disputes involving new media, especially the fast-evolving content on the Internet.

Get in touch: **cbarnett@scottandscottllp.com** | 800.596.6176