Responding to the Dreaded Software Audit

By Robert J. Scott

Modern financial history is chock full of embarrassing audit scandals, which caused executives and corporate brand names severe damage from intentional fabrication of revenues, or creating imaginary profits, or claiming assets that turn out to be a mirage.

There's a new scary cousin of traditional financial audits known as the software audit. It's increasingly become a threat to companies and their brands, often triggered by companies unintentionally violating very complicated software license usage terms.

The software audit notice brings a lot of challenges to the company being audited. They include potentially huge costs and penalties, legal liability and business risk.

Although challenging, there are measures a company can take to alleviate the impact of a software audit. Specifically, companies should put in place audit response policies to minimize the stress and financial burden of software audits.

Dealing with software audits is usually not a pleasant experience. Audits are time-consuming, stressful and potentially damaging to your bottom line. The scripts that auditors use to discover the illicit use of software (intentional or not) can themselves create problems in your IT infrastructure, consume valuable staff resources and money, and negatively impact your bottom line. And that's just for starters—simply because you pass one audit, that doesn't mean you won't be audited again in the future.

Here are a few key points to keep in mind when constructing your company's audit response policy.

- Even though vendors may have the contractual right to conduct an audit, make sure to check and see if the vendor's demand is consistent with the agreed-upon audit terms in your contract.
- You have wiggle room. There is always space to negotiate more favorable terms with the vendor because the vendor is usually interested in preserving the relationship.
- Just because legal and business interests have been threatened doesn't necessitate a legal response. But it's important to keep legal teams looped in from the very beginning.
- You should coordinate third-party auditor communications through your legal team throughout the course of any software audit inquiry.
- You should leverage pre-audit agreements to stipulate that the geographical and technical scope of one audit doesn't extend into all of your company's businesses and systems.
-

No one looks forward to software audits. In fact, they're about as popular as a wisdom tooth extraction. But a well-structured and well-thought-out audit response policy can ensure that every software audit you encounter ends in an optimal outcome.

Scott & Scott has defended over 500 software audits over the last 10 years. If you're interested in benefiting from our experience, reach out to us and learn how we help clients manage the risk of software audits.

About the author Rob Scott:

Robert represents mid-market and large enterprise companies in software license transactions and disputes with major software publishers such as Adobe, IBM, Microsoft, Oracle and SAP. He has defended over 225 software audit matters initiated by software piracy trade groups such as the BSA and SIIA. He is counsel to some of the world's largest corporations on information technology matters including intellectual property licensing, risk management, data privacy, and outsourcing. Robert ensures that Scott & Scott, LLP continues its focus on cost-effective strategies that deliver positive results.

Get in touch: rjscott@scottandscottllp.com | 800.596.6176