Supplier Audit Rights in Technology Agreements

Jim Steinberg and Lance McCord

Daily Report

August 7, 2015

In a recent article, we discussed contractual audit provisions that give the buyer of technology goods and services the right to verify that the supplier is meeting its commitments. In this article, we consider audit rights in the supplier's favor.

Suppliers typically request audit rights when key buyer obligations or supplier rights hinge on factors that would otherwise be invisible to the supplier. For example, suppliers' fees are often based on their customers' consumption of a product. Particularly in the case of on-premises software, a supplier does not have direct knowledge of the customer's consumption behavior (e.g., where license fees are based on the number of users, the number of instances of the software, the number of CPU cores, processing speed or other metrics known only to the buyer). Therefore, many software license agreements include audit provisions that give the supplier a right to verify the metrics on which license fees are based.

The risk to buyers of supplier audit rights is not always apparent. Certainly most buyers do not intend to violate the terms of an agreement and may not therefore object to the idea of allowing the supplier to verify the buyer's compliance from time to time.

But breaches can—and often do—occur. Buyer personnel responsible for software management may not understand the legalistic usage limits in a contract. Those responsible for procuring hardware may not be aware of the impact that hardware changes have on license counts (for example, where a license is for a limited number of processors or CPU cores). Licensed software may not be fully wiped from repurposed hardware. Or institutional knowledge concerning the use of licensed software may develop gaps over time as personnel changes occur. For all of these reasons, buyers should be wary when asked to agree to be audited.

The buyer's best option is to reject requests for supplier audit rights whenever possible. When it is necessary to accept a supplier audit provision, it is important to negotiate terms that create a fair process. The supplier should provide a reasonable amount of notice before an audit begins.

Keep It Confidential

All information disclosed by the buyer during the audit should be protected as confidential information that is provided solely for purposes of settlement. The agreement should impose a reasonable limit on the amount of time that the supplier and its third-party auditors can spend on the buyer's premises, and the supplier's rights should extend only to the information that the supplier needs in order to invoice the buyer correctly.

Suppliers often request broader rights, such as the right to verify buyer's compliance with restrictions on the use of the software. Such broad rights can make for a very disruptive audit. For example, most software licenses impose restrictions on the buyer's ability to produce copies of the software. It is impossible to verify a buyer's compliance with an anti-copying obligation without full access to the buyer's systems and records.

In addition to the scope of the audit, the parties must agree on how the audit will be conducted. For example, if an audit is intended to allow the supplier to verify a metric upon which maintenance fees are based, the parties should agree in advance on what will be counted and how.

It is not always clear what constitutes a billable resource unit. If license fees are based on the number of devices on which the software is installed, should the audit count a single computer running several virtual machines as a single device or several devices? Should decommissioned hardware that remains on premises be included in the count? If license fees for payroll software are based on the number of employees in the system, should the buyer be permitted to purge terminated employees from the system before the counting begins?

To address these and related issues, the buyer should attempt to include language in the contract that requires the parties to sit down before any audit begins and jointly agree on a process that will govern the supplier's and any third-party auditors' conduct of the audit.

The supplier's preferred audit process may include the use of audit tools—software that scans an IT environment for evidence of noncompliance. The buyer should reject the use of audit software because the buyer has no way to verify that the output from such software complies with the audit process agreed to by the parties.

'Environmental' Risks

Audit software may also present a risk to the buyer's IT environment. New software installed in a company's environment is typically subject to evaluation and testing and is backed by written warranties and indemnities that protect the company from the harm that defective or poorly designed software can do. Therefore, the contract should state that use of audit software is not permitted.

The contract should also impose limits on who will conduct the audit. If possible, the audit should be conducted by the vendor itself. But if the vendor wants the right to engage a third party, it is necessary to set some ground rules. The buyer will want third-party auditors to sign a nondisclosure agreement protecting the buyer's confidential information. The third-party auditor should not be engaged on a contingency basis—an auditor is more likely to find a problem when the auditor's pay depends upon it. In addition, the third-party auditor should be a reputable, independent firm (i.e., not an industry or trade association) so that information about the audit is not shared with other licensors who happen to be a part of the association.

When the audit work has been completed, the parties' first step should be an audit wrap-up meeting between the buyer and the supplier, where the supplier can share the results of its audit and supporting materials. Delivery of the audit results and supporting materials ensure that the buyer has the information it needs to dispute any part of the result with which it disagrees, and the meeting itself can help to expose errors or misconceptions underlying the audit results before the supplier issues a demand for damages.

If the supplier does demand damages based on the audit results, the damages should be based on the fees for usage of the software. Unauthorized use of software is infringement, and the supplier may seek to inflate its demand based on the statutory treble damages for willful infringement or punitive damages that it might be able to recover in court.

This approach ignores the fact that the parties have entered into an agreement that established a dollar value for the granted licenses. The buyer should seek to include the supplier's waiver of statutory and punitive damages in the contract.

Let the People Know

In addition to contract terms that ensure a fair process and a reasonable outcome, buyers should consider educating their personnel about how to recognize and respond to software audit requests. In many cases, audit requests are directed to nonlawyer personnel and framed in such a way that they are not recognizable for what they are.

A vendor's representative may reach out in advance of a license or maintenance term renewal to invite the buyer's personnel to install a small program that will ensure that the buyer is not paying for more licenses than the buyer needs. If buyer personnel agree to install the verification software, then an audit has begun without any discussion about process. By combining institutional awareness with carefully negotiated supplier audit provisions, buyers can minimize the risk posed by supplier audits.

A buyer is often able to leverage its relationship with its supplier's sales team during the audit process. When the supplier first requests an audit, buyers who reach out to their account representatives in the supplier's organization may find an ally in stopping the audit process before it begins. If an audit is conducted and the supplier issues a demand for damages, the supplier's legal team may be driven to obtain the best possible settlement for the supplier or to send a message to the marketplace that will make other customers think twice before violating the terms of their contracts with the supplier.

The supplier account representative, however, has the additional goal of satisfying sales goals and may be more disposed to a settlement that requires the buyer to purchase additional licenses, goods and services in lieu of paying damages. Therefore, the supplier should strive to make the first meeting following a post-audit demand letter a meeting between the buyer's business lead and the supplier account representative—without lawyers.

If the businesses are able to establish the framework of a settlement, then the lawyers can work to implement it.

Jim Steinberg, a partner at Kilpatrick Townsend & Stockton, focuses his practice on complex commercial transactions and general corporate matters for telecommunications, financial institutions, health care providers, technology and other companies. Lance McCord is an associate at Kilpatrick Townsend & Stockton, where his practice focuses on outsourcing and commercial agreements, technology licensing, advertising data and targeting agreements, joint ventures and strategic alliances.