HUNTON ANDREWS KURTH

Lawyer Insights

Key Readiness Tactics for a Software Audit, Part One: Software Audit Steps and Management

By John Gary Maynard, Andrew Geyer, Christina Edwards
Published in Business Law Today | December 7, 2022



The Great Recession taught an important lesson: if economic pressures prevent your organization from buying new software, then be on the lookout for an audit of your existing software licenses. Software vendors have seized upon noncompliance issues as leverage in convincing reluctant customers to buy new products.

For the past fifteen years, we have advised clients on how to manage software audits, even litigating when necessary. Over time, we've seen audits become consistently more sophisticated—employing well-known consulting firms, elaborate and tricky reporting mechanisms, and vendor-friendly scripts or automated review processes.

In this two-part article series, we will first delve into the steps of a software audit and tips for managing audits. Then, we will explore ways to improve your agreements to limit audits and put you in the best position possible when the auditor comes knocking.

PART ONE – STEPS OF THE SOFTWARE AUDIT AND HOW TO MANAGE IT

By John Gary Maynard, III

What should I do upon receipt of an audit demand?

When you receive an audit demand, there are several things you should do immediately.

Ownership. First, determine who will "own" the software audit. Is it your legal department or IT? The worst thing you can do is create ambiguity about who is managing the audit. You should also consider whether outside counsel should be engaged. Outside counsel can provide key advantages, particularly with respect to preserving privilege and avoiding admissions.

Collect Relevant Documents. At its core, a software audit is a contract dispute. Identifying and collecting all governing contracts and related documents is therefore imperative. If in doubt, collect it. Of course, there may be executed contracts between the parties that govern, but note that many vendors use clickwrap agreements. It may be difficult to obtain copies of these agreements, or even to verify through the vendor's website which version applies to your software. Don't forget that related documents, including settlements of prior disputes, may be set forth in emails or letters rather than in formal agreements. Vendors sometimes refer to these as "close letters." These can be crucial. Whether due to

the passage of time or sloppiness on the part of the vendor, it is not uncommon for vendors to present noncompliance fees based upon usage that was previously released.

Confirm Basic Terms. Although the terms of software contracts are as varied as the types of software, you should conduct an initial review of the relevant documents to answer the following questions: (a) which legal entities of the company are subject to the audit? (b) what is the geographic scope of the audit? (c) what software products are covered by the audit? and (d) what are the relevant deadlines? On that last point, you don't want to waive arguments by failing to respond in a timely manner.

Control Communications. Put procedures in place to control communications with, and about, the vendor. Establish a single point of contract, preferably someone with sound judgment and a good understanding of the business issues. We recommend a businessperson for this role rather than a lawyer. Once you've identified the single point of contact, notify the vendor and your employees. Guard against employees unwittingly making admissions regarding noncompliance. Relatedly, verify whether the vendor has any on-site personnel. If so, ensure your employees with regular interaction with the on-site vendor personnel do not talk about the audit.

What does the audit process look like?

Each vendor has its own process, but large vendors typically employ outside consultants as auditors. Shortly after issuing the audit demand, the vendor will likely introduce you to the auditor. Don't be surprised if the vendor does not participate in the audit from that point forward.

Kickoff Meeting. Once the auditor has been identified, you will be asked to participate in a kickoff meeting. There are several issues to consider before participating in this meeting, but, at a minimum, you need to confirm confidentiality of the audit. Your software contract likely contains confidentiality obligations between you and the vendor, but you likely will need a separate agreement with the auditor.

The Rest of the Audit Process. In general, the next steps will include: (a) an explanation of the data collection process, (b) collection of the data, (c) review of the data, (d) confirmation of the data by each party, and (e) monetization of any noncompliance issues. Each step is potentially fraught with peril. Whether you use inside counsel or engage outside counsel, it is imperative that counsel be involved at this point in the process, even though counsel likely will not communicate directly with the auditor.

How do I manage the audit process?

The goal with any audit is to resolve it with the least disruption to the company's business, and at the lowest price. Treating the audit as a business transaction, not an adversarial proceeding, is the best approach. Most vendors do not want to sue their customers. But this does not mean the audit process is not adversarial. Audits routinely identify alleged noncompliance issues, which vendors then attempt to monetize. The numbers can be extremely large—we've seen initial demands in excess of $100 million. Software agreements are simply too complicated for noncompliance issues not to arise. But those complicated agreements also provide opportunities for reasonable disagreement about the scope of noncompliance. It is a tricky process.

Role of Lawyers. Lawyers have important roles to play and should be involved from the very beginning. Obvious roles for lawyers include reviewing and revising confidentiality agreements with auditors, as well

as drafting any final settlement agreements or close letters. But the real value of lawyers is preserving privilege issues and avoiding admissions. At the outset, one way for lawyers to do this is to help business personnel establish reasonable parameters for the scope of the audit. Providing auditors with more information than they are entitled to rarely benefits the company. The single point of contact will convey the company's message in business terms, but that message will be guided by the terms of the relevant agreements that benefit the company.

Similarly, lawyers should help establish the parameters of the data collection process and the subsequent review of such data. This is particularly important for businesses in highly regulated markets. An audit should not unwittingly trigger regulatory breaches. Relatedly, several vendors use automated review procedures with prepopulated language that cannot be modified. These tools may appear to be an innocuous way to confirm usage information, but the prepopulated fields often contain admissions the company should not make. For example, the template might state all information is final and cannot be changed or modified. We've even seen some forms that have the company swear under penalty of perjury that the information is accurate and complete.

Finally, at the end of every audit, the business and its lawyers should work together to conduct a post-mortem. It is important to know if any noncompliance issues arose from inadequate internal controls. Any such issues should be addressed. Similarly, the company should consider whether technical problems or practices undermined or interfered with the audit. Finally, the company should also evaluate the vendor: was the vendor a good business partner during the audit? We once assisted a client who generated most of its revenue during a particular quarter. The vendor agreed to move the audit to prevent disruption during the company's busiest season. It was a simple gesture by the vendor, but it generated a lot of goodwill with the company.

Are there events within the control of the company that trigger an audit?

As previously noted, economic downturns can trigger audits. But other events that are within the control of the company can also trigger audits. For example, corporate restructuring can trigger an audit, because such restructuring may make changes to the identity of the licensed user. Most software agreements not only limit use to specific entities but also prevent an assignment to other legal entities—including affiliates of the original licensee—without the prior written consent of the vendor. Rapid growth can also trigger an audit. Most licensing metrics are tethered to the size of the licensee, such as the number of processors. Rapid growth, therefore, increases the incentive of a vendor to audit a licensee. Finally, nonrenewal of an existing software license can trigger an audit.

Final consideration: Not all licensed software is the same.

Broadly speaking, there are two types of licensed software. First, there is software that facilitates the operation of a business. Here, the business does not incorporate the software into a product that it sells but simply uses the software to make daily operations easier. For example, a doctor's office may use billing software in this way. Conversely, there is software that a company incorporates into its own product—the code that operates a vehicle's entertainment system, for example. Not surprisingly, this second type of software is typically unique. Audits regarding business operation software rarely result in formal litigation. It is simply in neither party's interest to formally litigate. Product-based software, however, can and often does result in litigation.

Key Readiness Tactics for a Software Audit, Part One: Software Audit Steps and Management
By John Gary Maynard, Andrew Geyer, Christina Edwards
Published in Business Law Today | December 7, 2022

With respect to business operation software, each vendor generally has its own licensing metric. Understanding that metric can go a long way toward identifying the likely focus of noncompliance issues. One common metric is the number of "users." This may seem like a relatively benign term, but disputes can arise over terms like "named users," "concurrent users," and "access." For example, with respect to the term "access," ambiguity in the agreement might allow the vendor to define a user as anyone with the ability to access the software as opposed to anyone who actually accesses the software. This definitional distinction could literally be the difference in millions of noncompliance fees.

With respect to product-based software licenses, it is difficult to generalize, because these are typically not off-the-shelf licenses that follow familiar patterns.

In any event, regardless of the nature of the software, the terms of the agreement will be crucial in determining noncompliance issues. In the next article, we will discuss ways to improve your agreements to avoid or limit an audit.

Key Readiness Tactics for a Software Audit, Part One: Software Audit Steps and Management
By John Gary Maynard, Andrew Geyer, Christina Edwards
Published in Business Law Today | December 7, 2022

John Gary Maynard *is a partner in the firm's Intellectual Property group in the firm's Richmond office. John Gary has a broad-based intellectual property and software litigation practice. He can be reached at +1 (804) 788-8772 or jgmaynard@HuntonAK.com.*

Andrew Geyer *is a partner in the firm's Global Technology, Outsourcing & Privacy group in the firm's Richmond office. Highly regarded in the outsourcing space, Andy Geyer handles complex domestic and international business process and technology-related transactions for clients in a variety of industries. He can be reached at +1 (804) 787-8164 or ageyer@HuntonAK.com.*

Christina Edwards *is an associate in the firm's Global Technology, Outsourcing & Privacy group in the firm's Richmond office. Christina is a trusted counsel to clients on all aspects of outsourcing and technology matters, including commercial contracting agreements, software licensing issues and managing high-volume transactions. She can be reached at +1 (804) 344-7911 or cedwards@HuntonAK.com.*