Planning for Recessionary Software Audits

MADISON ADVISORS

A Madison Advisors White Paper
November 2022

Let's be honest: the economy is slowing and inflation is increasing. Trying to maintain a level or even decreasing budget is going to be difficult for the next couple of years. And, if your organization is planning for a recession, it is safe to assume that your key technology vendors are modeling the same scenarios.

Throughout the world, raw materials, fuel and labor costs are increasing. In spite of this, companies have tried to maintain prices at the expense of profits. That strategy is no longer viable and companies across the board are going to need to raise prices. This includes the customer communications management (CCM) world. CCM software and consulting services costs will be rising over the next 12 months just so companies can maintain their own profit margins. If you are planning for a recession, you can be sure they are too and they will likely identify alternative revenue streams to drive growth in a downturned economy.

While raising prices for software and services predominantly impacts new and renewing customers, another way that software companies look to raise their income in a slowing market is through software audits. While you usually hear about companies like Microsoft, Adobe, etc. doing software audits, some CCM vendors may use the same tactics. Finding companies that have used too many licenses or have more servers than their contracts allow will be charged for going over those limits. At the very least, any breach will be used to renegotiate the licensing agreement and pricing.

This white paper outlines the two approaches to license management that software companies use and offers tips for successfully challenging audits. It also provides ways to avoid the time and expense of unplanned transactions in the future. License management is sometimes referred to as "entitlement management" as in you are "entitled" to this many seats, servers, pages rendered, etc., per the terms of your agreement with your suppliers.

TWO APPROACHES TO ENTITLEMENT MANAGEMENT

Every organization running technology has license agreements in place with their software and service vendors. These contracts define the type and amount of usage that is and is not allowed. The contract covers what a customer is entitled to use, and at what price, in the form of one or more of the following items: system access, environments, total output, volume, bandwidth, time, people, desktops, servers, queries, or other metrics.

Technical Compliance Approach

Some vendors use technical means to enforce compliance, which ensures the customer runs within the bounds of the agreement. In general, you will have transparent access to a portal or mechanism that grants access to the capabilities within the limits of the contract. For example, if you are licensed for 100 concurrent users, the 101st user will be denied access. If you are licensed to generate 10 billion communications per year, you will receive a system warning when you approach the limit alerting you that you are nearing the boundaries of your agreement.

Vendors that use a technical enforcement mechanism take on the burden of accounting for software usage by investing in access management. For the customer, this improves transparency and is usually accompanied by screens, portals or other usage reports that inform the customer of their usage. This approach removes the customer side burden and expense of audit compliance and risk of penalties for overuse. Using the data presented, customers reliably anticipate costs for any increased need in user licenses or output volumes before there is an unexpected hit to their budget.

Contractual Compliance Approach

Some software vendors strategically choose to rely on the contract as the enforcement mechanism. In this approach, customers have little to no obstacle, or alert, that prevents them from exceeding their entitlements. As a result, customers can unknowingly exceed the limits defined in the contract, without any warning. If a customer's access to the technology is not limited by the vendor, it is easy to add users, generate added output, or exceed usage allotments in a variety of ways that surpass the limits documented in the contract.

While the ability to use and access software without obstacles might be more convenient on a day-to-day basis, it can be difficult, or even impossible, to conduct a comprehensive inventory or usage assessment. This is especially true with the higher turnover of the Great Resignation, where named users may have left the organization, but their unused seat is still allocated or inaccurately checked back into the system. Not only does this lack of reporting and tracking create opportunities for the vendor to invoice you for hefty overages, but in this approach the vendor shifts the burden of contract enforcement to the customer. This is an expensive and time-consuming burden for a busy technology customer.

TIPS TO PREPARE FOR AN AUDIT

During downturns in the economy, it is common for software vendors that rely on the contractual compliance approach to increase the frequency and specificity of audits to their existing entitlement contracts. Each audit can trigger an unexpected six, or even seven, figure bill which will have to be justified to your chief financial officer (CFO).

If your vendor relies on customer-managed compliance to verify a contract, it is prudent to assume you will be audited. Here are some tips to prepare for these situations.

Before you are notified of an audit: Prepare

- Revisit your contract to clearly understand the boundaries in which you must operate to remain in compliance, or at least understand your exposure.
- Review your usage and remove unused logins, environments, or products to accurately match your usage to your access.
- Pay specific attention to user licensing requirements. Named users are the most difficult to audit, so they should be reviewed periodically to ensure they are consistent with the current license user's identity.
- Calculate usage using any reporting mechanisms you have available to compare your usage to the contractually defined metrics.
- Understand the rights and obligations of all parties in case of an audit, especially the period covered by the audit to prevent a lookback if not explicitly included in the contract.
- Consider your communications with the vendor if they rely on the contract for support. Your answers to apparently innocuous questions about usage, output, or access may be preserved and interpreted as evidence of a breach of contract. Atypical communications may be the first step in an audit process.
- Create a communication plan that establishes a single point of contact during the audit to ensure you have awareness of all communications with the vendor to avoid your team members being played against each other.

During the audit: Remain in control

While you need to cooperate during an audit, you do not have to do your vendor's work for them. Shift as much of the burden of proof onto them as possible, ensuring that any auditing scripts or software, data access policies or records request do not conflict with your customer guaranteed or government-mandated data privacy policies.

- You, and your security team, control what, if any, license tracking software is deployed. Your IT partners, and governing legislation, may allow you to refuse to install tracking software.
- Understand whether you must comply with a backward-looking audit or one that is a snapshot in time. Vendors with contract enforcement will benefit the most from going back as far as possible, but the contract may not require you to comply.
- You may not have to accept their estimates as evidence of usage. You may be able to demand detailed reports of alleged breaches of an agreement from your vendor.
- Consider the value of an audit non-disclosure agreement (NDA) to both parties before signing. Seek to strike any non-disparagement and non-disclosure language from an audit NDA to reserve your right to share your experiences freely in the market as a bargaining chip in case of a settlement.
- Demand detailed accounting that is objectively verifiable by both parties. If you are told you have significant communication or file-size overage, demand to see the logs that prove which applications, systems, users and environments are responsible. Also find out when those occur. Shift this burden to your vendor.
- If there are file size overage charges, compare your file sizes to other similar technologies to ensure they are within acceptable industry standards. You shouldn't be paying extra for large files that result from a vendor's architecture choices.

HOW TO MINIMIZE THE IMPACT OF AN AUDIT

If you have gone through one of these software audits in the past, you may not want to repeat the experience. There are some actions you should take to avoid this in the future.

- In your requests for proposals (RFP), ask questions about contract enforcement, likelihood of an audit and ask if the vendor has received license revenue from non-compliance in the past three years.
- During the selection process, expand the circle of roles accessed for reference calls to include finance, legal and procurement professionals from customers with over five years of implementation experience.
- Ask if the vendor relies on technical enforcement or contractual enforcement to protect the intellectual property (IP) of their software.
- Be prepared to leave your vendor by ensuring that all your design, logic, data and delivery IP that you've invested in their solution is retrievable in a readable form at any time from the vendor. This will allow you to switch to another vendor, if needed.
- Demand to see how they provide real-time reporting to you of your usage against the contract terms, to reduce the time and energy you spend on ensuring compliance.
- Ask if there are entitlement warning mechanisms, like when a mobile carrier sends a warning that a customer has used 75% of their monthly data allotment.
- Consider leaving an anonymous review about any audit policy, experience, or settlement that you consider to be unfair on a public review site. Take care to omit exact numbers and identifying information about your company.

CONCLUSION

Software audits are a reality that businesses of all size need to be prepared to handle. Reviewing existing contracts and license agreements prior to an audit can save time associated with an audit and help mitigate any penalties associated with contract breaches. As more and more software companies are acquired by private equity firms, software audits are seen as a quick way to generate revenue. By being prepared with both data and a unified front to the software provider, companies can minimize the impact on their bottom line.

© Copyright 2022 by Madison Advisors. Madison Advisors, Inc. All Rights Reserved. All other product names are trade and service marks of their respective companies. This publication and its contents are the property of Madison Advisors, Inc. No part of this publication may be reproduced or duplicated without the express written consent of Madison Advisors, Inc.