SURVIVING THIRD PARTY VENDOR SOFTWARE AUDITS

Tobi Mott
tjmott@hollandhart.com

HOLLAND&HART

SOFTWARE AUDITS ON THE RISE

The Stats

- Nearly 70-80% of licensees will be audited
- Average of 3 audits per year, 2-3 months to complete each
- Over 50% result in true-up costs
- Almost 20% exceed $1 million
- 75% admit that fear of audit increases odds of over-licensing

Why?

- Continued use of legacy enterprise applications
- Strategy to enhance revenue for enterprise software vendors
- Increasing audit activity in cloud environments
- Software easy to install on multiple devices
- Complex licensing terms and models

WHO IS AUDITING?

IBSMA Survey (International Business Software Managers Association)

Top 10 Vendors

- Adobe (phased out audits in most markets)
- Attachmate
- Autodesk
- HPE/MicroFocus
- IBM
- Microsoft
- Oracle
- SAP
- Symantec
- VMware

Increasing Audit Activity

- Cisco Systems
- Citrix
- Google
- McAfee
- OpenText
- Quest Software
- Salesforce.com
- Tibco

AUDIT NOTICE

SOFTWARE LICENSE REVIEW NOTICE

[Client] has been a valued [Vendor] customer and we hope that our products have been instrumental in your organization's success. On behalf of your [Vendor] account team and staff, we thank you for your business.

[Vendor] periodically performs software license reviews with its customer base of thousands of organizations. These reviews not only help us better understand how our products are used, but also provide invaluable information to our customers to ensure that their software deployment remains compliant with the license grant.

In this direction, and pursuant to your Software License Agreement and the audit rights and obligations contained therein, we hereby notify your organization of our intent to perform a software license review.

Once our review is initiated we will discuss procedural details and determine the best timing for various engagement activities. In order to ensure that everything is performed in the least disruptive manner possible to your team, we will work to accommodate your busy schedule. However, we would like to complete our review no later than within 30 days of the receipt of this letter.

Within 3 days of receipt of this letter, please contact our Engagement Manager within our License Management Program, [contact info] acknowledging your receipt of this letter. A nationally recognized audit firm will be utilized to complete the review. Once receipt has been acknowledged an introductory meeting will be scheduled between all parties. During this meeting, we will explain the proposed scope of the review, the actions you will be required to carry out, and the estimated timeline for completion.

We would like to thank you in advance for your collaboration during this process.

EXAMPLE - TIBCO SOFTWARE AUDIT

- Provides middleware and business process management software
- Used heavily by investment banks
- Example of software vendor with aging product portfolio and aggressive approach
- Targeting smaller entities to extract revenue since less likely to sell more software
- Recently settled claim against GAIN Capital
  - TIBCO originally sought $22 million additional fees
  - Alleged breach of contract, breach of implied covenant of good faith and fair dealing, and copyright infringement
  - GAIN disputed KPMG's deployment report
  - Counterclaims for fraud and negligent misrepresentation

FIRST STEPS

Initial auditor meeting

- Vendor proposed reliance on existing confidentiality terms between client/TIBCO and TIBCO/KPMG
- Outlined audit process and roles

Submitted NDA

- Rejected existing confidentiality terms, Client has particular confidentiality considerations
- Used NDA to negotiate audit scope
- Attached client's data security policies to guard against intrusive audit

Internal deployment analysis/risk assessment

- Reviewed existing license agreement and order forms
- TIBCO was not able to produce updated entitlements
- IT team used SAM tools to identify all deployments and compare to entitlements

TIBCO AUDIT CLAUSE - 2010

21.9 Licensee hereby grants Licensor, at Licensor's expense, the right to appoint an independent third-party auditor to audit Licensee's compliance with this Agreement no more frequently than once per year, upon reasonable notice and at reasonable times during normal business hours.

Prior to accessing Licensee's equipment or facilities the auditor will sign, and thereafter abide by, Licensee's safety, security, and privacy policies, including executing an appropriate non-disclosure agreement with Licensee.

Licensor shall require the auditor to consult with Licensee in making a final determination in good faith as to (i) whether any undisputed discrepancy exists between the Number of Units licensed and the Number of Units used by Licensee; and (ii) the amount of such discrepancy. Licensor shall abide by the findings of the auditor.

For a three (3) year period following the initial Order Form Effective Date, the parties agree that in the event an audit reveals an overdeployment of Number of Units of the Licensor Software, Licensee agrees to pay Licensor license fees for such additional Units as follows:

So long as the overdeployment is less than fifty percent (50%) of the total Number of Units of the Licensor Software set forth in Section A.1 above, Licensee shall be granted a discount of seventy- five percent (75%) from Licensor's most current list price for such additional Units, plus applicable Maintenance fees, based upon discounted list price license fees.

If an overdeployment exceeds fifty percent (50%) of the total Number of Units of the Licensor Software set forth in Section A.1 above, Licensee shall be granted a discount of forty percent (40%) from Licensor's most current list price for such additional Units, plus applicable Maintenance fees , based upon discounted list price license fees.

By way of example,

If Licensee has licensed 8 Processors of TIBCO Enterprise Message Service but has deployed 12 Processors of TIBCO Enterprise Message Service, Licensee will pay for 4 Processors of TIBCO Enterprise Message Service at a 75% discount from TIBCO's most current list price.

Licensee's payment of the fees described above are Licensee's entire liability and Licensor's sole and exclusive remedy for Licensee's overdeployment of the Licensor Software.

- Reliance upon 3rd party auditor
- Right to require NDA and compliance with policies
- Ability to provide input
- Interesting overdeployment language

AUDIT SCOPE - PHASES

TIBCO Software Discovery

- Internal SAM discovery using KPMG list of keyword queries, plus self-report any software not covered by SAM
- Completed KPMG's Software Inventory Form for servers and developer workstations only where TIBCO software is "running"

** Note that client rejected KPMG's automated scripts for security purposes*

TIBCO Software Data Collection

- KPMG interviewed:
  - Software Asset Manager
  - Hardware administrator re hardware specifications where TIBCO software was running
  - TIBCO Administrator to verify the number of users with the ability to access the TIBCO software
- KPMG inspected hardware to capture screenshots showing installed TIBCO software

** Limited KPMG's unsupervised access to people and systems on-site*

AUDIT SCOPE - PHASES

TIBCO Onsite Data Validation & Testing

- Accuracy Testing: verify the TIBCO software products reported by the automated tools are actually running on the machines through use of screen shots
- Completeness Testing: verify the machines that do not have TIBCO software products are indeed not running TIBCO software
  - KPMG asked client for a list of all active servers/workstations that do not have TIBCO software
  - KPMG randomly sampled to confirm no TIBCO software is running on the sample machine through use of screen shots

Reporting/ Closing

- KPMG compiled all data and prepared a draft deployment report, no comparison to entitlements
- Client had up to 21 business days to review the draft deployment report
- Client had chance to provide written feedback for KPMG to incorporate into the draft deployment report
- KPMG released draft deployment report to TIBCO
- TIBCO added in the corresponding entitlements
- Project closing meeting, “3-way call”, to review the final report
- KPMG then steps out of the process
- Client and TIBCO finalize a settlement

KEY NON-COMPLIANCE RISKS

- Straight up overdeployment
- Complex licensing terms and models
- Virtualization
- Rogue employee actions
- Indirect access by third party applications
- Shared accounts, multiple logins, multiple devices
- Incorrect categorization of users
- Bundling restrictions
- Sloppy decommission practices
- Global deployment, misunderstanding country restrictions
- M&A transactions
- Procurement disconnect from legal

LEVEL THE PLAYING FIELD

- Attack the audit clause
  - Notice periods, time to conduct internal review
  - Frequency of audits, no more than once every 12 months
  - Audit scope: snapshot in time vs. look back
  - Direct vendor vs. independent, third-party auditor
  - Require confidentiality terms
  - Compliance with licensee data security requirements
  - Audit costs, limit to third party out-of-pocket if underpaid by 5-10%
  - Prenegotiate license fees and maintenance costs to avoid current list prices

- If negotiation isn't possible, hold vendor to a limited interpretation of the word "audit"
  - Limit to review of existing records re software usage, reject full investigation of IT systems
  - Remote vs. on-site
  - Snapshot in time only
  - Leverage general confidentiality and data security provisions

Don't forget the underlying commercial terms

- License definitions and usage rights, attach separate policies to contract
- Installed vs. running
- Legacy entitlements vs. new master license terms, avoid the trap of references to new online terms and policies in ordering documents
- Order of precedence