Software License Non-Compliance and Audits: Growing Hazards and New Action Items

Compliance and Ethics

Technology, Privacy, and eCommerce


SOFTWARE AUDIT


SOFTWARE AUDIT

CHEAT SHEET

- ***Why us?*** Vendors believe that audits are necessary to protect their significant investment in their intellectual property. Some customers, however, believe that it is easier for vendors to increase their revenue and margins by auditing existing customers, rather than closing new license sales with new customers.
- ***Realistic, but proactive.*** The best way for a customer to limit its potential liability for software non-compliance is to be proactive and attempt to prevent any potential violation of the license grant. Consider implementing, and periodically updating, a comprehensive software procurement and use policy, as well as conducting regular employee education on that policy.
- ***Self-audit.*** Companies should seek the right to conduct a self-audit and then provide the vendor with a pre-specified, limited degree of information, and/or documentation based on the results of the self-audit.
- ***The request.*** Upon receipt of a vendor's audit request, a company should engage with their sourcing and legal teams to identify and find applicable license components; understand the terms of the applicable licenses; examine the purchase history with the vendor; and track the actual, documented compliance with the license terms

Gotten audited yet? Has your client suffered the disruption, uncertainty, and costs of being accused, reviewed, and surprise-invoiced by its software supplier(s)? It's likely you will.

Dozens of unpublicized litigations, large-money unplanned "true-up" payments, and other recent-years disclosures illustrate the relatively new and often-overlooked, difficult, and growing risks associated with on-premises software license administration and software license audit clauses.[1]

1 This article focuses on "on-premises" software licenses, where the software is loaded on computers owned or controlled by the customer. This architecture differs from "software as a service" (SaaS), where the software is run at the vendor's site on its hardware or at a third-party site (and customer data is therefore distant too).

Too often, IT managers, procurement personnel, and even attorneys focus solely on the terms of the initial transaction license grant when licensing software. They mistakenly underappreciate and ignore audit clauses as mere "legal boilerplate," unlikely to arise and irrelevant to business priorities. In the past, that might have been true.

Today, however, these assumptions are shortsighted as such business myopia ignores and conflicts with recent changes in the software industry, carrying significant risk to licensees. The necessity for both organizations and counsel to actively and vigorously address on-premises software license non-compliance risks and audit clauses is illustrated by recent multi-million-dollar settlements, unexpected payouts, protracted lawsuits, and more software vendors adopting aggressive, programmatic auditing and litigating.

For example, Anheuser-Busch InBev (AB) recently disclosed in its annual shareholders report that global software vendor SAP is seeking more than US$600 million from AB in arbitration. SAP claims that AB employees directly and "indirectly" used SAP's software without appropriate licenses.[2]

Discovery pleadings disclose that one vendor, Attachmate, set an internal sales quota of US$100 million for its team of “compliance managers” — all of whom were law school graduates — in their “checkups” with incumbent customers.[3] Over US$100 million was sought in an “intra-industry” claim; a leading software company was accused and sued for alleged over-deployment by another software company, plaintiff Phoenix Technologies.[4] In England, Diageo is defending the damages portion of a lawsuit filed by SAP, seeking approximately US$54 million in damages, having been found to violate the license grant scope in old contracts from SAP.[5]

This article will explore both why software audits happen, at all; why many software vendors are becoming much more aggressive in initiating and conducting detailed, distracting, often contentious software “compliance audits”; and the contracting, intellectual property, compliance, and business continuity risks associated with such audits. It will then discuss the significant issues and options associated with reviewing, drafting, and negotiating audit clauses in software licenses and practical, effective steps to mitigate the varied audit-associated risks.

2 Anheuser-Busch InBev SA/NV Form 20F for fiscal year ending December 31, 2016, p. 154, filed March 22, 2017 with the US Securities and Exchange Commission.

3 The revenue quota covered four software vendors under common ownership (Attachmate, SUSE, NetIQ, and Novell). Transcript of February 6, 2015 deposition of “compliance team” manager Darren Rice (pleading 128-7 filed September 8, 2015 in now-settled *Saks, Inc. v. Attachmate* [Case cv-04902-CM-RLE, US District Court for the Southern District of New York]), referenced in *Fidelity National Financial, Inc. v. Attachmate Corporation v. Black Knight Financial Services* (June 15, 2017 declaratory judgment plaintiff’s and third-party defendant’s brief opposing vendor’s summary judgement motion) (Case #: 3:15-cv-01400-HES-JBT, U.S. District Court Middle District of Florida [Jacksonville]).

4 Licensee/defendant VMware argued that its supplier misread the license scope, and was merely mining for extra unearned revenue, in bad faith, after receiving new funding, strategy, and instructions from new investors. After two years, VMware won a jury verdict of no liability. (June 12, 2017, Pleading 438, NDCA #: 3:15-cv-01414-HSG).

5 The parties litigated a 2004 base contract with 2009 and other amendments, many years later. *SAP UK Limited v. Diageo Great Britain Ltd* [2017] EWHC 189 (TCC) February 16, 2017. Such long, multi-years latency is common in enterprise software license interpretation, disputes, and audits.

Technology and business context: Why are audits continuously necessary?

Audits are a common aspect in technology licensing in general and software licensing in particular for a number of reasons:

- Many on-premises software transactions are “self-service.” The licensor supplies a “master” copy of the software that the customer easily copies, distributes, and loads onto its computers.[6]
- Software “delivery” is usually plural — an ongoing, iterative event. New product features, bug fixes, and changes to improve interaction with other software and hardware all cause the initial software to differ from what is deployed later.
- Unauthorized copying and use is a significant revenue and survival challenge to software

companies. “Broken” use-privilege keys, “cracked” security filters, and bootleg copies are well-established injuries to vendors’ finances.

- Even if not “piracy,” many users do not understand the rights and obligations of the companies for which they work. As a result, they do not know how to ensure that their use of software is consistent with the underlying contract.
- Software contracting often is deficient. The technologies, business processes, and contract terms of ongoing software deliveries leave lingering, often significant questions. Frequently “business as usual” software-handling fails to yield clarity, precision, and good recordkeeping among customers regarding both usage rights and what software has been loaded or is being used in the customer’s infrastructure.
- Industry insiders admit that customer software management is a challenge in which gaps are frequently found. Staffing, tools, and reporting regimes are missing or weak as often as they are present or robust.
- Audits do identify customer confusion, and improper use.

6 Some software transactions are explicitly and intentionally “pay-as-you-go.” They provide for a periodic (usually annual) calculation of recent use and resulting possible supplemental payment, known as a “true-up.”

Prohibition on licensor auditing the number of licensee users: Licensee oriented

Based on the enterprise scope of license rights, the parties agree that there is no need for, and licensor shall not request, an audit of licensee. If licensor believes that licensee is in violation of the license grant provisions, licensor can request a written compliance certificate, in writing, per the notices provision of this agreement, specifying licensor’s (i) requested data items (by date, media, and technical attributes) and (ii) reason(s) for requesting, provided that neither such request nor any actual delivered certificate shall modify this agreement or create a separate cause of action.

Why are software audits increasing in recent years, in frequency, intensity, and initiating vendors?

The increasing number of software audits is a reflection of the changing nature of software licensing. The software industry is transitioning aggressively from paper-only, easily stored and reviewed licenses to only or primarily electronic browse-wrap and click-wrap licenses. Moreover, virtual contracts (or contract components) often “reside” only or primarily on a vendor’s website. Often, such terms can be unilaterally or intermittently modified by the licensor, so license obligations now — unlike in the past — reside in a complex blend of paper and electronic documents and components. These disparate pieces span many years, and have usually never been studied or integrated by IT, procurement, or legal into one easily understood document. Often absent is a single interpretation shared by both the vendor and customer.

Second, inadequate software-specific contracting skills and efforts place many customers at a clear disadvantage in a complex software-licensing environment. Ambiguous license terms are often not addressed during negotiation/procurement, particularly fee-bearing “indirect access.”[7] As a result, the customer will not fully analyze and understand what it agreed to until a dispute arises. Many times,

IT, “sourcing,” and/or finance personnel are deployed who can skillfully handle procuring unchanging physical goods and supplies or simple services, but who have never studied the nuances, history, litigations, or particular risks associated with procuring a morphing, mixed product-and-services need like software. Further, busy generalist lawyers often lack the time to develop domain-specific expertise.

7 *See, e.g., SAP UK Limited v. Diageo Great Britain Ltd* [2017] EWHC 189 (TCC) February 16, 2017 and many US and non-US litigations involving Attachmate. See, e.g., *Epic Systems v. Attachmate* (Case 3:15-cv-00179-bbc, U.S. District Court for the Western District of Wisconsin [Madison], generating 223 pleadings during March 19, 2015 - July 25, 2016) and *Sherwin Williams v. Suse et al.* (Case 2:15-cv-00129-JNP-DBP, US District for the District of Utah, generating 109 pleadings during February 27, 2015 - October 31, 2016).

Vendors believe that audits are necessary to protect their significant investment in their intellectual property. Too often, customers either intentionally or unintentionally exceed a license’s use restriction. Without a right of audit, vendors would never know if a license’s use restrictions had been violated. Some customers, however, believe that it is easier for vendors to increase their revenue and margins by auditing existing customers, rather than closing new license sales with new customers. “Enterprise” software is an industry now more challenged than in the past by customer alternatives such as “open source” software, new products based on newer software design techniques and programming languages, and competitors in lower-cost countries.

Audits often identify customer non-compliance — and hence new invoices and revenue for vendors. Customers’ breaches of their software supply contracts frequently result from the complexity, variety, and ongoing iterations of software licensing documents. Moreover, vendors’ changing licensing and pricing models (e.g., on-premises, core-based, seat license, concurrent user, and other variations) cause contract administration, interpretation, and integration challenges that many procurement departments do not identify, undertake, or handle with questionable precision.

Acquisitions, mergers, reorganizations, and spinoffs by customers can transgress “anti-assignment” clauses in end-of-contract “boilerplate.” Many software vendors monitor merger news and initiate audits — and efforts to “upsell” new licenses and services — to such customers in transition. Customer consolidations also create challenges in tracking and complying with license obligations. Post-merger cost-cutting and reductions in force often undermine both the inability to find old contracts and limit funding for staff and specialized software tools to assess and document compliance.

Finally, a technology gap exists. It is industry consensus that there is no easy, proven, or single solution to enable customers to identify what software has been deployed and the applicable use limitations. True, software “asset management” and “discovery” products are available that allow parties to identify and inventory their software. However, these products can be expensive and potentially cumbersome to configure, install, populate with data, and later update. “False positive” and “false negative” outputs from self-discovery tools can require supplemental manual inventorying.

Confidentiality of audit

Each party agrees to hold confidential (in accordance with Section _ (“Confidentiality”) all information created, aggregated, or learned and all determinations made in the course of any inspection, “discovery” activity or audit under this Section _ (“Audits”), except solely when it is necessary, and to the extent, for a party to reveal such information in order to enforce its rights under this agreement

in arbitration or in court and except when compelled by law.

Elements of an audit clause

Prudent practitioners should carefully review and negotiate audit clauses in every software license, both to limit the customer's risks and the cost of ongoing compliance, and to protect the licensee from aggressive licensors seeking to maximize revenue and margins. Every audit clause should be carefully considered from the perspectives of cost and potential disruption to the customer's business. The following are common terms in an audit clause and corresponding considerations.

Frequency: Most customers seek to limit the vendor's audit rights to only once in each 12 to 36 month period, arguing that there should be no need for a vendor to audit more frequently.

Notice: The notice of audit initiation should set forth in detail both (1) the specific process and nature of the audit and (2) the particular software that the vendor seeks to audit. Customers should have a reasonable, specific duration (e.g., a minimum of 30 days) to respond to an audit request, and then an additional, longer specified duration (e.g., a minimum of 60 days) to prepare for the audit. Preparation — which usually requires significant efforts by the customer, including identifying and organizing records of deployment and/or usage, and often finding and hiring specialist outside firms — should allow the audit to occur with less confusion or ambiguity. The customer should also have the right to postpone the audit for a good faith reason. (i.e., the year-end closing financial books may justify a delay.)

Hours: Audits should be conducted only during normal business hours. Seasonal businesses may want to strive to exclude their respective "busy seasons."

Location: The audit location(s) will depend on the nature of the audit. Most audits are initially conducted electronically by running a software tool on the customer's computer hardware to identify any non-compliance with the license terms. Also, a vendor's hired CPA firm's staff or employees often wish to supplement, validate, and/or interpret electronic inventorying results with additional, on-site (1) sample testing of selected computer servers, (2) interviewing IT and/or procurement personnel, and/or (3) project team meetings.

Duration: Prudent customers seek to place a time limit on the length of the audit (e.g., 30-45 days) to attempt to limit the disruption and operational cost.

Cost allocation: Traditionally, the audit-initiating vendor assumes all of its audit costs, including fees of any third-party auditing firm, unless the audit identifies a specified level of under-payment (e.g., five percent). Further, the vendor does not typically reimburse the customer's costs in (1) deploying staff, (2) procuring specialized inventorying software, and/or (3) hiring outside specialist "audit defense" technology consulting firms and/or specialist legal counsel. Any reimbursement should be limited to the vendor's reasonable out of pocket fees paid to an outside CPA or specialist consulting firm, excluding vendor staff and overhead. Also, a "fee-shifting" provision — triggered if the audit does not result in some minimum payment — might be appropriate.

Auditors: Many customers require the use of an "independent" third-party auditor. The wisdom of this requirement is illustrated by disclosures in some litigation that vendor "compliance" personnel

arguably were undisclosed salespersons, rather than neutral experts (e.g., since they were "reporting up" within the sales function, carrying minimum revenue quotas, and/or receiving bonus payments for generating additional revenues). Third-party auditors should be required to sign a non-disclosure agreement and should have agreed upon minimum qualifications for conducting the audits. Note that the professional standards of independent certified professional accountants (e.g., AICPA rules in the United States) do not apply to such software audits. Customers should exclude third-party auditors being compensated on a contingency basis based on the quantum of identified underpayments, as has long been the contracting norm in audits in other copyright and license based industries.[8]

8 In recent, pending litigation, a defendant-customer argued that a global "Big 4" CPA firm failed to meet the contractual "independent" auditor requirement due to the large quantity of software audit work that the CPA firm had received from, and other relationships with, the particular software vendor.

Tools: Vendors uniformly use software tools, often of their own making, to identify believed customer non-compliance. The vendor should be required to demonstrate the accuracy of the tool and provide traditional representations, warranties, and indemnities consistent with any other software that the customer installs. Also, consider whether additional special, granular requirements are appropriate, given increasing (1) inclusion of internet-born open source software in all commercial software, (2) well-publicized worries regarding malware and belated identification of security bugs, and (3) regulatory requirements of network security. At a minimum, the vendor should be required to comply with the customer's IT/cybersecurity standards and indemnify the customer in the event of a breach of those standards. Moreover, since some vendors now include tools in their software to unilaterally, automatically detect and "report back" apparent or actual unauthorized usage — whether explicitly permitted in the license agreement or not — cautious customers will include warranties regarding specifying when the tool's use must be concluded. Customers should seek advice from its network security team and its outside consultants, to help define specific technical processes and standards for prior review and authorization of audit-function code.

Audit subject: The audit should be limited to confirming the customer's payment obligations. Alternatively, the audit clause should clearly identify and limit what the vendor is permitted to audit, to prevent the vendor from searching for potential opportunities to sell different or more software and/or identify any competitor software used by the customer.

Audit period: Vendors should be limited to auditing the customer's payment obligations only for the lesser duration of (1) since the last audit concluded, and (2) a specified, negotiated calendar duration (e.g., one year, though vendors will seek more). In no event should vendors be able to go back more than three years.

Compliance with customer policies: The vendor, the vendor's auditor, and their respective employees should be obligated to comply with all applicable customer policies, such as those governing network security, site physical security, and perhaps background checks of the vendor's (or vendor's CPA) staff.

Compliance with laws: To the extent the audit may provide the vendor with "protected data," the vendor should be contractually obligated to comply with all applicable laws such as data privacy laws in the European Union and elsewhere.

Confidentiality/use of audit results: All aspects of the audit, including the results and any reports, should be used solely regarding the audit and should not be disclosed publicly in any manner. See

the sidebar below for a model confidentiality clause.

Top 10 considerations for planning and preparing for an audit

1. “One riot, one ranger” is an obsolete frontier mythology: The necessary education, experience, and expertise to plan and execute a proper audit response (or defense) rarely is possessed by any single individual or department. Collaboration among multiple operational groups and functions is mandatory. Finding and utilizing outside experts and consultants is typical and smart.
2. Software is special (hard): Your supply chain colleagues rarely handle any purchase with so many changes and intangible (electronic) pieces. So expect unfamiliarity and variation from any so-called “purchasing norm” and complexity.
3. Process controls: IT experts are invaluable for operations, but are unqualified to independently handle often subtle, contentious, expensive contract compliance interpretations, investigation, and negotiations.
4. Crosswinds of change: The global trend of electronic contracting makes it especially challenging to assess contractual obligations covering both legacy paper and more recent virtual era transactions. Expect identifying, integrating, and interpreting multiple contract pieces to be a challenge particular to software licensing and audits.
5. Think plural: Often, several licenses apply to the same product during the relevant duration (e.g., due to multiple versions). Usually the analysis must consider not “the contract” but “the contracts, over time.”
6. The devil is in the details: It is not just software itself that is characterized by unending minutiae (i.e., the underlying code). So too are inventorying results. Loaded software usually lacks standardized, easily electronically searchable “tags” and varying pricing rules often apply to evolving software products and versions. Thus, audit outputs regularly require rigorous, iterative cross-checking in order to identify “false positives,” link data and dates to sequential versions of the same software product, and determine which versions and terms of the vendor’s license(s) apply.
7. Big money and IT dependence merits preparation: Since large-gap audits may yield seven and eight figure USD true-up demands, per organizations’ reliance on software availability, and given plenty of audit-specific litigations, structure self-audits upfront to merit attorney-client privilege. Hire and manage self-audit specialized technology consultants only via counsel, not IT, especially for first time audits where ambiguities and disputes are foreseeable.
8. Bad news does not getter better with old age: If a problem has been identified, it is best to be forthcoming with the vendor after a complete and counsel co-managed self-investigation, instead of merely hoping that the vendor will not “find” the problem.
9. Realistic expectations about process and outcome: This may hurt for months. The vendor has planned, executed, and collected cash from its audits many times before. Expect gaps, ambiguities, frustrations, new tasks, and friction with each new audit.
10. After invasive surgery, close the wound: Leverage the occurrence to yield both better procurement and ongoing compliance going forward — especially since vendors frequently re-audit customers in later years (and vendor salespeople may “leak” good targets to other vendors’ personnel).

“True-up” pricing for over-use of software: The price for any software that the customer must license for over-utilization identified by the audit should be per pricing specified in the underlying prior software license(s). However, some vendors’ contracts specify higher or later, undefined “then-current” pricing for such compliance remediation. These vendors sometimes specifically ban (1) “true-ups” via purchases through the customer’s usual reseller and (2) the application of any prior or current discounts from suggested list price.

Interest: Some vendors’ standard contracts provide for the addition of the highest-available level of interest (e.g., 12 percent per annum, per Washington state law, in many Attachmate contracts and litigations).

Permitted overages: Prudent customers who plan well their software sourcing negotiations will seek to include language allowing them to exceed the number of purchased licenses by a specified amount (e.g., five percent) before interest or penalties would apply.

Release: Upon conclusion of the audit, all payments should be contingent on the execution of a mutual release, in full satisfaction of all liability the customer may have to the vendor.

Addressing and mitigating the risk

Be realistic, be proactive

The best way for a customer to limit its potential liability for software non-compliance is to be proactive and attempt to prevent any potential violation of the license grant. Waiting until the vendor has requested an audit is too late.

It is important that the customer both (1) implement — and periodically assess and update — a comprehensive, specific software procurement and use policy and (2) conduct regular employee education as to the policy and the importance of compliance. Uninformed, overly flexible, or “rogue” software licensing will not end well for the customer. It is especially important to educate the IT, procurement, finance, and legal teams regarding recent-year changes in software license models, the placement of license terms in multiple locations by vendors (i.e., that important pricing, rights, and other terms may be found only on vendors’ web sites, or may change without notice after the initial contract signing), and expected audits. Adequate software sourcing training now should include the catalysts, contentions, costs, chaos, and concessions evident in dozens of US and many non-US audit-specific litigations, since those pleadings reveal “do’s, don’ts, and ‘this could be you, but don’t let it be’ lessons” in real-world, dramatic detail.

Ban risky “client self-surgery”

Procurement and IT teams should be prohibited from responding to vendor audit requests or pre-audit “inquiries,” and even from conducting their own self-audits, without the involvement of the legal team. IT staff often blithely comply with supposedly low-key, “business as usual” questionnaires or “usage queries” from software suppliers, unaware that the resulting data may be initial evidence and the first step in an incoming painful project. As to full-on audits, many entities have found that naïve, embarrassed, or under-managed IT personnel have attempted to “take care of it internally,” viewing that all software issues are their exclusive province. Such personnel usually lack the contract interpretation, intellectual property law, vendor dispute, and other training and experience to identify and optimize the organization’s response and results.

Procurement and IT teams should be prohibited from responding to vendor audit requests or pre-audit “inquiries,” and even from conducting their own self-audits, without the involvement of the legal team.

Moreover, smart customers will strive to structure the audit and its results to merit the protection of the attorney-client privilege (at least within the United States) particularly for litigious vendors, first time self-audits, and situations of suspected non-compliance. Audits often uncover ambiguities, possible “smoking gun” emails (e.g., staff complaining about the software buying process, record-keeping, or budget constraints), and premature admissions that can and do undermine vendor negotiations and optimal resolution.

Further, outside technology consulting organizations hired by IT leaders to help prepare for and defend against vendor audits often fail to educate or urge their sponsors to structure the project to report to and through the legal function. Just as in audits for possible non-compliance in labor, environmental, securities, or other legal domains, outside specialists should be contracted by the legal department to enable possible protected nondisclosure of potential “bad news.” Prudent practitioners should check the laws of the governing jurisdiction to determine whether external IT consultants being hired by and reporting to outside counsel, rather than the legal department, is necessary in the jurisdiction to obtain protection under attorney-client privilege.

“Preventive law” includes check-ups

Every entity should conduct annual software use self-audits to assess and hopefully confirm its compliance with its frequently evolving contractual obligations. Identifying potential problems in advance may allow a customer to resolve an issue with less cost, risk of license termination, risk of reputational damage (e.g., from litigation), and disruption prior to the vendor possibly becoming aware of the customer’s non-compliance. Further, some vendors look more favorably on customers who self-report their non-compliance. As noted above, regarding the frequent need to deploy outside technical specialists, any self-assessment should involve the customer’s legal department to protect the results through attorney-client privilege if available.

Propose alternative audit mechanisms

The most favorable solution for the customer is to exclude an audit provision from the license agreement, perhaps linked to a one-time large transaction or older, nearing-obsolescence software. The customer’s ability to do so, however, is unlikely in most settings, given the vendor’s desire to protect its intellectual property.

Alternatively, the customer should seek the right to conduct a self-audit and then provide the vendor some prespecified, limited degree of information and/or documentation based on the results of the self-audit. The feedback provided to the vendor can take several forms: (1) a certificate provided to the vendor, (2) a summary of the audit findings, or (3) the actual audit findings.

Regardless of the format of any audit, it is important that the customer and vendor agree on the specific process and tools that will be used to conduct the audit. By agreeing to the process and tools, the customer will be able to prepare for, and limit the extent of, the audit and the vendor’s ability to conduct a fishing expedition.

Responding to an audit request

Upon receipt of a vendor's audit request, a prudent customer immediately should engage with the customer's sourcing and legal teams to:

- Identify and find applicable license components (which likely will have evolved from the initial license agreement, and usually takes more time, effort, and stress than initially predicted!);
- Understand the terms of the applicable license(s) (often a significant, iterative struggle, given the cascade of changing products, pricing terms, and contracts);
- Examine the customer's purchasing history with the vendor; and,
- Track the customer's actual, documented compliance with the license terms.

In the customer's initial response to the vendor, the customer should limit its correspondence to letting the vendor know that they are preparing a researched, reasoned response. Savvy customers will research and seek insight on the particular vendor's history and approach in prior audits of other customers.

Failing to cooperate with a vendor's audit request provides no value from a legal perspective. Vendor-filed lawsuits often include dramatic, detailed stories of customer "stalling" when contractually required audits have been refused.

The customer (as a team with the legal department's inclusion) should:

Quantify: Thoroughly examine the audit data with the goal of validating any claimed overages. Often ambiguities are found and must be assessed — or negotiated — regarding (1) the meaning of terms in old, or even recent, contracts, (2) which audit tool outputs are actually accurate, and (3) which licenses, from which years, apply to which product versions, from different usage times.

Interpret: Once the internal data is collected on usage patterns etc., the audit response team must vet the data against the governing license terms. Sometimes ambiguities in the vendor document might explain or arguably "excuse" wrongful use. A lack of clarity in the license language, however, often works to the vendor's advantage in the context of vendor-driven audits and associated threats of license termination.

Negotiate: Simultaneous with such diligence, the project team should engage its supply chain team to help maximize any leverage to be gained from the customer's business relationship with the vendor. Additional data on current expenses and anticipated future purchases from a software supplier often increase the customer's leverage when negotiating, depending on the vendor's then-current internal priorities and financial cycle.

Defend: Once the believed cost of any confirmed overages is independently determined or estimated by the customer, the customer should act (1) defensively based on its internal investigation, and (2) offensively based on leveraging the parties' future relationship, to attempt to ensure a settlement with the lowest possible cost.

Conclude: Once an agreement has been reached, a release should be executed between the parties.

Optimize: Once the totals and alleged costs have been confirmed, the customer should assemble supporting data internally as to how any actual overages occurred so that over-utilization does not

arise again in the future.

Conclusion

Software audits are becoming increasingly more common as vendors are becoming more aggressive in efforts to increase their revenues and margins. Prudent customers should both scrutinize, “de-bug,” and modernize both initial software intake and ongoing lifecycle management, and carefully negotiate the terms of the audit clauses in their agreements to ensure they are protected from both a legal and business perspective.

The authors welcome and encourage comments on the analysis and recommendations in this article.

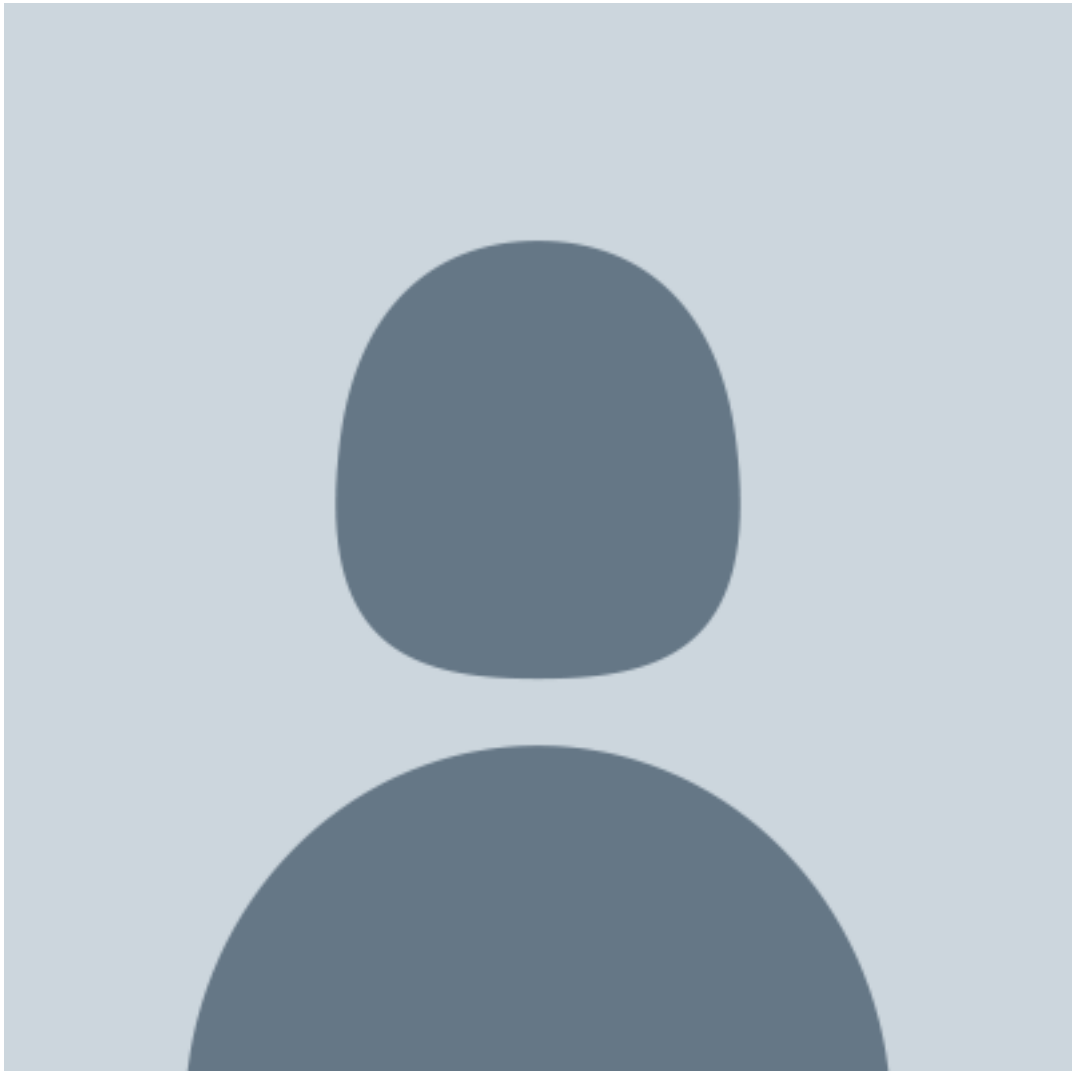
H. Ward Classen

General Counsel

Astea International Inc.

He is the author of A Practical Guide to Software Licensing for Licensees and Licensors (ABA Press, now in its sixth edition).

Henry W. (Hank) Jones, III



the law office of Henry W Jones, III and Intersect Technology Consulting

He formerly served as head in-house counsel of two global publicly traded technology vendors, and as VP, IP development for a third. For 37 years, he’s focused on IT issues, including transactions, risk mitigation, disputes, and corporate training.