

IAITAM *is* ITAM



*International
Association of IT
Asset Managers*

*Professional IT Asset Management
Certifications – Consumer Advocacy – Solutions
www.iaitam.org*

Defusing a Software Audit

International Association of IT Asset Managers
500 Grant Street
Akron, Ohio USA 44311
Info@IAITAM.org

Defusing a Software Compliance Audit

Contractual Breach = Non Compliance, Litigation, Punitive Action, Piracy...

Global corporations are paying the price for ineffective management of software assets. As software sales continue to taper off and corporations reduce IT spending, the software publishers have been required to more closely monitor the configurations of corporate computing systems for license violations. Let's face it: we've been on a buying frenzy – acquiring the “latest and greatest” operating systems and software with little consideration for strategic planning or life cycle management. ROI? Isn't it obvious that there is currently no effective process for tracking ROI on software or many other IT assets? Configuration management? We've relied on consultants and a highly mobile IT work force to load / configure software on systems – a work force that may not be closely tied, ethically, to our company and one that frequently moves on, leaving very little detailed knowledge of the work completed. Where are all the software packages located? We don't know because the people who put software on our systems are frequently no longer with us.

License compliance management documentation? Companies have no idea where many of these documents are all located – or even if they still exist. Moreover, many enterprise accounting standards actually dictate a policy of destroying records after 3-5 years. As a result, the average IT division has no formal documentation process that precisely details the software products it possesses, the location of where that software is configured / loaded / stored or if those applications configured are even still in use. Yet deep within virtually every major software license agreement are clauses giving the copyright holder the right to demand that we conduct compliance audits & report the results. More to the point, we are also required to be capable of producing the related compliance proof of purchase documentation on demand – even though that requirement may not be clearly detailed in our license contract. The time couldn't be more ripe for us to become targets for non compliance litigation.

This document is a general review of some of the issues that led us to where we are today: A point in time when compliance enforcement has become big business operating on a global basis. Those corporations that have found themselves targeted for non compliance litigation were, and are, defenseless due to their utter lack of effective software asset management processes and procedures. This brief paper will discuss some of the issues leading to negative compliance enforcement events followed by a series of basic recommendations for initiating change in the enterprise to reduce exposure. The International Association of Information Technology Asset Managers (IAITAM) believes it is time to “Educate – Don't Litigate – Compliance.”

What *IS* compliance?

Simply put: Compliance *should* be “the degree to which the consumer and supplier adhere to the terms and conditions of the mutually agreed-upon license document.” Please note that IAITAM stresses the software licensing process should be a two-way street. Not only are you responsible for compliance but so, too, is the software publisher. Unfortunately, the vast majority of software licenses offer no definition or details regarding compliance expectations. Most licenses merely state that the “publisher, or its representatives, may conduct an audit for compliance.” This lack of detailing brings us all to an enhanced potential for non compliance across the life cycle of the copyrighted product and, often, beyond. Essentially, the rules governing compliance are constantly changing. Due to changes in the industry and the way in which we actually use our systems & software, compliance requirements differ from time to time as well as publisher to publisher. This “floating compliance” concept tends to place the corporate consumer in a position of continually **reacting** to compliance assurance processes rather than proactively managing its assets across their respective life cycles.

For the purposes of this paper, we will define compliance as follows: “Compliance is the clear documentation that the number of legally obtained & genuine software licenses matches the number of a given product configured on computing devices” in the organization. Further: “The consumer is responsible for maintaining complete and accurate records of all license documents. These records include, but may not be limited to: the actual license, certificates of authenticity, proofs of purchase and master media. Other strategic documentation may be added as necessary, but only if agreed upon in writing. The software publisher / copyright holder must clearly define compliance requirements – including necessary documentation.”

In addition, it is critical that you define the length of time documentation must be retained. One of the major reasons that many companies lose compliance audits is that they cannot locate their documentation. As noted, various accounting departments recognize differing requirements for retaining documentation ranging from three years to the seven required under Sarbanes-Oxley. As a result, destroyed documentation can become a major issue. Remember: Contracts are supposed to be mutually beneficial agreements between two or more parties and a software license is a contract. This concept is must be kept in mind during your interactions with the software publishers who have developed the products your company uses on a daily basis. You absolutely must work to negotiate not only a license agreement, but also a very clear understanding of how that agreement will actually function. That agreement must detail compliance assurance.

How do you become a target?

Corporations become targets of compliance enforcement entities through multiple pathways. Primarily, the enforcement industry relies on toll free confidential telephone lines and web submissions. Their messages encourage employees; current or former, disgruntled or ethical, to alert the industry watchdogs of a non compliance issue. Other resources utilized by the software industry can include your competitors, suppliers and consultants: Virtually anyone who can communicate credible knowledge of your organization can push you into a negative confrontation with an enforcement entity or copyright holder. Once targeted – unless you are completely prepared – you WILL lose.

What should you do when you become a target?

Primarily, you should NOT panic and begin reacting indiscriminately: Believe it or not this is a very common reaction. A second inappropriate reaction is for companies to assume that an immediate, open and honest admission of full guilt will help their case. Please remain very aware that these compliance confrontations are not initiated unless they are based upon a strongly assumed clear knowledge that your organization is not utilizing software products according to contractual Ts & Cs. The only effective reaction to a compliance threat is to carefully prepare your case and negotiate intelligently from a position of strength. Companies that fail to approach a compliance audit in a strategically planned manner will not win.

First, create and clarify a communication process to manage the compliance event. The corporate software asset manager should work directly with legal counsel to develop a step by step process to move all compliance-related communications quickly through the corporate infrastructure. This means that whoever receives a non compliance notice knows – up front – that they must immediately forward the notice to corporate legal counsel and to the software asset manager. The recipient of the notice must never communicate with the compliance enforcement entity and must act quickly to place the communications into the hands of the appropriate personnel.

Executive Task Force

The next step is to convene a high level Executive Task Force dedicated to overseeing all tasks necessary to mitigate or eliminate the threat. The Task Force should include the CEO, CFO, CIO, legal counsel, software asset manager and other individuals deemed necessary by the corporate culture. Permit no observers – this is an action group, not a spectator event.

The Executive Task Force is responsible for developing your eleventh hour action plan. Or, preferably, this group follows the proactive action plan for

IAITAM *is* ITAM

countering a compliance audit event – a plan developed as part of an ongoing enterprise process to manage this potential risk event. The Task Force is not a forum for placing blame or for internal confrontation. Instead, the group functions as a focal point and resource to enable the audit processes to take on the priority necessary to protect the corporate entity from a very real and potent external threat. Permit the Task Force to populate and guide the various Action Teams that will move through the corporate infrastructure gathering strategic compliance assurance information. Action Team managers report to the software asset manager who reports progress to the Executive Task Force.

Enterprise Action Teams

Action Teams can be composed of a single person to a small group – they are dependent upon the complexity of the enterprise environment. Teams are cross-functional so individuals can be part of any or all teams. Function is critical as well as the speed of collection and accuracy of results. Recommended teams would include:

- **Documentation Management Team** – Locates, details and reports core numbers of all software-related documentation. "Here is what we are permitted to have."
- **Configuration Management Team** – Conducts an automated audit of all computing devices to discover software configured / loaded on systems. "Here is what we actually have."
- **Reconciliation Team** – Receives all totaled counts from both other teams. Determines, documents and reports overages or shortfalls. "Here is where we are short or over."

Rule One – Recognize, and make clear to the Executive Task Force that you may, indeed, have violated your license agreements. Review every license to identify all relevant terms and conditions that apply to your situation. Again – remember that the license is a legal contract between your company and the software publisher. If you have violated the agreement, you could be considered to be in breach of contract unless you pre-negotiated terms into the contract protecting your company from non compliance litigation. Always keep in mind that the software publisher is within its contractual rights to confront non compliance.

Rule Two – Only legal counsel is permitted to discuss the issues with the compliance entity. Also, legal is only permitted to discuss details from your perspective AFTER the corporate action team has met to produce a preliminary compliance status report based upon factual data – not verbal assurances. Legal counsel does, however, have a certain responsibility to narrow the exposure through preliminary discussions with the compliance enforcement entity. This preliminary discussion can take many forms but its major focus is to clarify and narrow the accusations being made regarding the specific software titles under investigation.

IAITAM *is* ITAM

Rule Three – Everything is negotiable in these confrontations. Compliance enforcement entities settle the vast majority of non compliance issues out of court. If your counselor is thoroughly prepared with accurate background knowledge and strategic information they will be much more capable of protecting your interests through negotiations. Giving the legal department or person a well-supported negotiating position will move your company forward into a much more tenable position. The alternative is almost certain defeat.

Rule Four – Do not, under any circumstances, delete software or modify systems configurations when you are under a formal audit notice. In many cases, this type of action can be considered spoliation of evidence and could easily escalate the action being taken against you.

Preliminary Discussion

Counsel must first review the corporate position with the Executive Task Force. This is a critical step in that it helps provide the individual counselor with the multiple reference points from which to begin, and on which to base, the coming series of interactions with the enforcement entity.

Primarily, counsel needs to become clearly aware of the precise content of the actual enforcement letter / communications. Based upon this information, the corporate software asset manager briefs the counsel on the approximate status of the corporate compliance repository. This should take the form of a very simple listing, by software publisher, of all products the corporation believes it possesses; the approximate numbers of licenses, certificates of authenticity and proofs of purchase for each product; the number of computing devices present; the date and details of the most recent configuration audit; the count of assumed configurations for each product; the names of the audit tools in use and their currency; a list of corporate compliance policies including any disciplinary actions relating to violations and other documentation as considered necessary. It will also be necessary to conduct a full review of all applicable software license terms and conditions at this time.

This information should bring counsel and other Executive Task Force team members up to speed very quickly. As well, it provides counsel with a very powerful potential foundation for entering into discussions in a controlled & confident manner rather than as a defenseless victim.

The early discussions between counsel and the compliance enforcement entity should include corporate counsel requesting clarification of the precise accusations against the company. Counsel wants to:

- Deflect the potential event altogether through demonstrating how completely prepared the company is for a compliance audit. If the company is maintaining an effective – accurate & timely – software asset

IAITAM is ITAM

management program (including compliance assurance), there is a very good chance counsel will be able to eliminate the threat in the initial discussions. This requires advanced planning and attention to detail but effective preparation can enable the company to nearly eliminate compliance audit threats before they pick up litigation momentum. An effective lawyer, equipped with accurate strategic compliance assurance information, should be capable of bringing resolution to the compliance question or at least severely limiting the threat at this point.

- Narrow the threat field - If the company does not have sufficient strategic information, it is even more necessary for counsel to narrow the threat field during this first communication. Essentially, according to historical patterns, the compliance enforcement entity will provide a broad list of software publishers whose products are suspected as being utilized outside of licensed terms. Conversely, many software publishers investigating non compliance will request or demand an audit of their entire range of products – often a huge number of irrelevant titles. This list should be narrowed as much as possible. Legal counsel must negotiate disclosure of specific products for each publisher in question. The more the list can be narrowed, the lower your actual exposure with a corresponding reduction in the amount of documentation you will be expected to produce.
- If your company has developed a strategic document content management system, you will also be capable of providing legal counsel with synopsis details of compliance terms and conditions from all software licenses maintained on site. This knowledge is critical to your defense.
- If time is an issue, counsel should take this opportunity to lobby for an extension on the deadline for producing the completed audit.
- If the company is not prepared for any form of audit, do not admit it at this time. Merely clarify the issues and begin preparations for building your defense from whatever strategic information you are able to locate. Unfortunately, this is precisely where many companies begin the process.

While the processes above are being addressed the Action Teams do not remain static. The Executive Task Force's absolute core purpose in these events is to take as much of the event control and momentum as possible away from the compliance enforcement entity. Your company should focus on remaining out of "enforcement action reaction" mode and well within the "standard compliance reporting" mode.

Begin, immediately, preparing the Status Report.

Preliminary Compliance Status Report

Documentation – Initial Status

At this point in time, what is the company's precise status in regards to documentation and actual compliance-related configurations? As noted, one of the core reasons so many companies lose non compliance confrontations is because they cannot locate the documentation supporting their claim to legal possession of the copyrighted product. Where are all the proofs of purchase, certificates of authenticity, licenses and other supportive documentation? What is the precise number of each copyrighted product that you are permitted – by license – to have in your environment?

If this material is centrally located and detailed, providing the accurate totals at this time will help your counsel negotiate. If not, provide as accurate a number of permitted licenses as possible and immediately move to the formal documentation process recommend in this briefing.

Configurations – Initial Status

What software is actually present on your corporate computing devices? As part of the compliance event you are required to conduct an audit of your computing devices to demonstrate the count of various copyrighted products loaded / configured on each device. Although some compliance enforcement entities will reluctantly accept a hand audit, note that the accuracy of hand audits is always questionable.

For the preliminary status report, most companies may only provide legal with an accurate estimate of this number. If, on the other hand, you already have accurate, automated configuration information, you are capable of providing clear answers at the beginning of the interaction. This will usually enhance your position with regard to the potential settlement.

Reconciliation – Initial Status

For the preliminary report, you will need to provide legal counsel with the total number of copyrighted products you are permitted to have present compared to the total number of copyrighted products you actually have present on systems as well as on the shelf. Comparing the two numbers will provide an initial snapshot of your license overage or shortfall.

The Preliminary Status Report is a microcosm of the over-all compliance report. While the preliminary report provides immediate information, the over-all report process develops your actual detailed compliance assurance documentation. This documentation is, or must eventually become, the basis for the corporate software life cycle asset management program.

Next Step – Formal Documentation Process

License Documentation & Purchase Summary

This document – usually a spreadsheet – details the total number of each licensed product that your company is contracted to have in its possession. It should detail the following:

- Software Publisher Name
 - Product name or names in your environment produced by this publisher
 - Versions or releases of each product under licensed agreement?
 - How many licenses are present?
 - How many Proofs of Purchase are present?
 - Cancelled checks, paid invoices and etc.
 - Vendor reports documenting sales to your company.
 - Are the Certificates of Authenticity present? How many?
 - Is master media present?
 - Is other license related documentation present? List.

It is strongly recommended that you never send the originals of this documentation to the compliance enforcement entity. Although you will be asked to do so, losing control of your originals is contrary to good business practices. Negotiate this point.

Product in Use Summary

This document, again in spreadsheet form, details the total number of each product found to be present on each computing device in your environment. It should detail:

- Software Publisher Name
 - Product name or names produced by this publisher configured on systems
 - Total number of each product / version / release found present

Licensed Product Shortfall or Excess Summary

This document details the reconciled numbers of legally licensed product against the total number of products actually located on the specified audit site. The count may show that the company has an excess of licenses or it may show a shortage. Again, it is most effective if broken down by software publisher, followed by product & release or version.

Product Detailing by Computer

As you audit your systems, you will be creating a snapshot of the hardware configuration of each computing device as well as the operating system and software present on that device. Formalize and maintain this document for future use. The actual report will consist of each computing device within the company, followed by the list of all products found on the device sorted by publisher. This report will be valuable to you should you discover a shortage – it will enable you to locate all given software product targeted for removal or replacement. The report detailing product by computing device should not be released to any outside entity.

Non Compliance Audit - Reactive Synopsis

IAITAM recommends the following broad reactive steps in addressing a voluntary audit communication. Please note that IAITAM does not provide legal advice or legal negotiations recommendations – always clear every action with legal counsel before initiating the action. A simplified reactive process:

- Communicate only through qualified counsel,
- Understand that the copyright holder has the legal right to monitor compliance as defined by its license,
- Remain 100% honest and ethical in your actions throughout this process.
- Do NOT throw yourself on the mercy of the entity. It will not be beneficial in any manner. Conversely, do not antagonize the entity: cooperate but remain non committal and firm,
- Do not yield to intimidation: know your rights in an audit event,
- Ensure that executive management is directly involved in the process,
- Require that the enforcement entity minutely detail its accusations. Expect specifics regarding publishers' products involved in the investigation. This is a tough requirement but it is necessary,
- Know & understand your licensed rights regarding compliance and an audit. Remain firm in negotiating a mutually beneficial closure,
- Do not attempt to “go it alone.” The software and license enforcement industries are organized and multifaceted. Defense against threats of litigation requires that enterprises and legal counsel work together to construct a mutual strategic process. Consult with IAITAM to gain access to other companies & legal personnel who have been in this position. Communication will be extremely beneficial in helping reduce the number of mistakes made during this process,
- Acquire and detail quantifiable evidence regarding acquisition and possession documentation, including -
 - All licenses,

IAITAM is ITAM

- Proofs of purchase,
- Certificates of Authenticity,
- Master media,
- Vendor sales confirmation reports,
- Manuals & other documentation as considered necessary.
- Conduct an automated audit of computing devices as detailed by the enforcement entity. Compile detailed documentation regarding –
 - Precise count of all systems and servers,
 - Detail whether thick or thin client,
 - If thin client, detail the linkages to software accessed from servers,
 - All copyrighted products present on systems,
 - Detail by software company, versions & releases,
 - Detail by computer – then by software publisher & product,
 - Know and document the precise numbers of each product present.
- Create an audit report including –
 - The product list as requested by the enforcement entity,
 - Total number of each product for which you have documentation,
 - Present and missing documentation for each product.
 - This is your list of “what the company should have.”
 - The total number of product located on all computing devices,
 - Sort by publisher and product, then version,
 - Document precise numbers.
 - This is your list of “what the company does have present on your devices.”
- Reconciliation document
 - Document, listed by publisher (copyright holder), followed by product, noting the difference between what you should have present and what you do have present.
 - This is your overage or shortfall report and is the document most referred to in negotiations.
- Document the numbers of thin clients and precisely what servers each thin client or client server desktop accesses,
 - For each, document the software products accessed on the server or servers,
 - Provide any metering information the company might maintain.
- Key issue: The more detailed and complete your documentation, the more effective will be your defense. This material is what your legal counsel needs to negotiate against the enforcement entity. Most companies that lose these encounters do so because they failed to track this information.

Software Asset Management

Once you have completed your compliance audit it is critical that you formalize the process and continue to perform compliance-related reviews of corporate systems. Usually, any settlement for non compliance requires your company to be prepared to produce current compliance audit results for a period of up to three years. If you maintain this process, you will be able to do so.

More importantly, the processes and procedures you have just implemented for a compliance audit are the cornerstones of an effective – proactive – IT asset management program. IAITAM believes it is critical that you understand that maintaining such an accurate and timely system will enable you to lower your life cycle costs for both software and hardware through more effective use of strategic information.

Documentation - Ongoing

For compliance - You must be capable of producing license documentation, in an organized manner, upon request. As noted, although you should never relinquish possession of the actual files, the enforcement entity will lead you to believe this is required – negotiate this requirement out. The format of your presentation of this material is usually a basic table document showing the software publisher name, product, version/release, and numbers of permitted configurations detailed by each document in your possession.

Quality and volume of documentation are negotiable issues in the compliance event. However, you must have access to the actual documents so legal counsel can refer to or utilize them, when and if necessary, in your defense. Ensure that counsel is knowledgeable in interacting with a compliance enforcement entity.

Configuration - Ongoing

IAITAM recommends that you utilize an automated discovery tool (discussed in the IAITAM briefing: “Choosing & Using a Configuration Management Discovery Tool”) to review every computing device and document – automatically – your precise numbers of configured copyrighted product. Filter and detail this information by publisher, then by product lines within the publisher’s offerings. Generate automated, but filtered, configuration reports. It is strongly recommended that you never provide raw, unfiltered reports to a compliance enforcement entity.

Reconciliation - Ongoing

Once you have collated all license, authenticity and purchase documentation, you will have a list of products you are entitled to possess. This list will include the precise number of each product you are permitted to have configured on corporate systems.

IAITAM is ITAM

Within your discovery tool reports, access the number of actual configured products and match this number against the number of products you are licensed to have present.

If you have more products configured than you are permitted by license, you could be out of compliance. This is what the compliance enforcement entity is hoping will be the case. In fact, in the vast majority of compliance enforcement events, this IS the case.

The reconciliation report is the document upon which most compliance enforcement actions depend for closure. Make certain this document is accurate and clearly defensible.

Closure

This briefing tends, by necessity of its delivery method, to be incomplete in its coverage of reactive compliance. Every enterprise is unique and will require slightly differing preparation in these events. IAITAM Professionally Trained & Certified Software Asset Managers (CSAMs) have reported that the specifics of negative compliance enforcement actions also tend to differ from company to company. This is due to many factors: degree of strategic compliance data preparation, quality & quantity of documentation, corporate culture, economic positioning, corporate size, focused experience of legal counsel, knowledge of the SAM team and more. Any single document will be incapable of addressing your precise options and opportunities.

This document is meant as a starting point – a basic foundation on which to build at least a partial defense. Additional information may be obtained through joining IAITAM, participating in the IAITAM List Serve and Forum, attending IAITAM focused training programs and becoming / remaining proactive in your asset management procedures.

IAITAM members do not believe in nor advocate an “us versus them” mentality in working with the software publishing, compliance enforcement or hardware industries. We do, however, function as a consumer advocate. IAITAM has resolved to work toward building a mutually beneficial relationship between customers and suppliers – a relationship that has capacity well beyond its current levels. The suppliers of goods and services for the IT industry work hard to develop the most effective products possible. They have a right to a positive return on that investment. Conversely, the consumer also has a right to receive due consideration in product and service quality. If we work together to provide that mutual benefit we will all emerge on the winning team.

IAITAM Certified Software Asset Managers (CSAMs), Certified Hardware Asset Management Professionals (CHAMPs) and Certified IT Asset Managers

IAITAM is ITAM

(CITAMs) are professionally trained in their focus areas. They are committed to participating in an ongoing continuing re-certification program that requires them to remain current in their knowledge and functionality levels. IAITAM, the association, represents the IT consumer on a global basis in methodologies for proactively managing IT assets – software, hardware, support & maintenance as well as service contracts - across the life cycle. IAITAM certified professionals, properly supported by their enterprises, do not guess about compliance – They have strategic knowledge based upon quantifiable enterprise statistics.

Currently, corporations have multiple choices:

- They can choose to not manage their IT assets,
- They can attempt to manage their IT assets without proactive training and method,
- They can obtain unfocused training (training developed for other purposes and modified to apply to IT). This training usually has little ongoing support or follow up,
- They can obtain training developed by “special interest groups” (training focused on selling additional services or products). Support for this training is usually either unavailable or comes with ongoing acquisition strings attached,
- They can obtain training and support developed by professional IT asset managers FOR professional IT asset managers – IAITAM training & support.

Don't go it alone. IAITAM is your global community of IT asset management professionals. Refer to other IAITAM briefings for additional life cycle management knowledge.

No Legal Advice

Please be aware that the information above is provided for informational purposes only, may not reflect the most current legal developments, should in no way be taken as an indication of future results and is not offered as and does not constitute legal or any other advice on any particular matter. No one should act or refrain from acting on the basis of any information contained in such responses without first seeking the appropriate legal or other professional advice on the particular facts and circumstances at issue.

This document is governed by the IAITAM arbitration / mediation policy as posted on the IAITAM web site: www.iaitam.org.