

How to Survive a Software Audit through Effective Software Management

By John Tomeny, Sassafras Software Inc.

According to the October 2002 “U.S. Software State Piracy Study” published by the Business Software Alliance, one out of every four software applications used in the United States is unlicensed. The subject of software piracy, and how software is pirated, was commonly misunderstood by many a few years ago. But vigorous efforts in recent years by two software industry trade associations, the Business Software Alliance (BSA) and the Software & Information Industry Association (SIIA), and by individual software vendors have improved the level of awareness – if not understanding – on the issue.

The BSA reports that within the United States in 2001 losses from corporate software piracy were approximately \$5.7 billion. However, this doesn't tell the full story. Both the BSA and the SIIA indicate that the losses experienced from “Internet piracy” and piracy of game software and entertainment software by individuals would substantially inflate these numbers. Some industry analysts refute such estimates, claiming that the real revenue loss from piracy by individuals is low. They argue that the bulk of software pirated by individuals does not have much actual value to the person who pirated it. Hence any calculation of lost revenue relative to a purchase price is spurious – a legitimate purchase would not happen unless prices were reduced.

Keith Kupferschmid, Vice President of Intellectual Property Policy and Enforcement for the SIIA, asserts that the estimated \$5.7 billion figure for corporate piracy is accurate given his belief that companies would purchase the software they used if it wasn't pirated. So what is pirated software anyway? How can we best define it in the ‘corporate’ context? Does each copy of an application found on each computer drive – whether the machine is currently in use or in storage – count? Does each have to be licensed? What about dormant software that is installed but unused on a computer that is in regular use? If a software program has not been launched for a considerable length of time (months or years) does it still need to be validated by a license? These are all questions we will explore in this paper.

What are the Common Forms of Piracy?

Since we are exploring your organization's 'corporate' risk, we will ignore commercial counterfeiting activities and other piracy that occurs outside of the corporate setting.

In the workplace, employees often share software with each other without going through proper channels to obtain licensed copies. Or they sometimes bring personal copies from home to work and load them onto their computers. These acts of piracy are often done with little or no forethought about anything other than the need to accomplish their work on schedule. Employees look for the most convenient way of getting things done. They also sometimes download unlicensed software from the Internet. All of these forms of piracy can put your organization at risk.

Other acts of piracy can take place within an organization when the company expands or changes personnel. The licensing details can be forgotten or overlooked during times of change leading to negligent and illegal copying and installs. Additionally (and especially in times of economic downturn) organizations might engage in deliberate cost cutting practices that lead to unlicensed use of software.

Pirated software is not simply software that has been counterfeited for resale, but includes any unlicensed use of software by individuals in any setting. But, thankfully, there are effective tools available today that your organization can use to protect itself from legal exposure and risk. We will examine them in a moment. First, let's take a closer look at the "policing" organizations.

Who are the "Software Police"?

The Software & Information Industry Association was originally founded in 1984 as the Software Publisher's Association. With over 800 member companies, it is the principal trade association for the software and digital content industry. The SIIA participates in government relations, serves as an industry advocate, provides continuing education opportunities, and protects the intellectual property rights of its members.

The Business Software Alliance was founded in 1988, has approximately 20 member companies, and is focused primarily on activities to protect the intellectual property rights of its members. Both organizations provide toll free hotline phone numbers for reporting of unlicensed use of software. Additionally, the BSA carries out an active, roving "grace" campaign designed to reduce the use of unlicensed software and boost sales for their member companies.

Their members endorse both organizations to represent member interests at customer sites. They are empowered to request – and carry out – software audits

under copyright legislation and/or by specific language in software license agreements. Their empowerment is validated by corporations' desires to avoid threatened legal action.

What is a Software Audit?

There are two common types of audit requests that your organization might receive either from the BSA, the SIIA, or directly from a software vendor. The more common – and more benign – of the two is typically initiated by an informational letter that explains the merits of using licensed software and encourages the reader to download a free software audit tool to run on their site.

This is the approach currently used by the BSA in their roving amnesty campaigns. In their campaign, the BSA will provide additional instructions on how your organization can participate in their program. Typically they will inform you that for your organization to participate, you must not have previously received notice from the BSA or its members of suspected software license infringement within your organization. There also must not have been any prior warning of investigation. Finally, prior to or during their grace period your organization must have acquired sufficient software licenses to ensure legal use of their members' software.

The second – and much more serious – type of request that can be initiated by either organization or by a software vendor is a direct request that informs you of suspected software license infringement within your organization. As the SIIA's Kupferschmid explains, "If a company gets a letter from us you can bet that we already have pretty extensive information."

How Should My Organization Respond to a Software Audit Request?

As the saying goes, "An ounce of prevention is worth a pound of cure." The best approach is to do the work of becoming compliant in advance so you will not have to be worried about how to respond in the event that you do receive an audit request. We will explore a suggested step-by-step plan in the next section. As you read the plan, the important principal to keep in mind is to 'buy the software that your organization uses and throw away the rest'. It is always better to do this in advance rather than when under pressure.

What Can We Do to Reduce Our Risk of Legal Exposure?

First you must understand what the auditors will be looking for. In the context of corporate or educational piracy, here is the short list:

- End User Piracy (staff/students installing and sharing unlicensed copies)
- Client-server Overuse (unmanaged server access)
- Internet Piracy (staff/students downloading unlicensed software)
- Hard-disk Loading (vendors installing unlicensed "gifts" to new computers)
- Software Counterfeiting (not typically found in educational or workplaces)

Next, you must eliminate these forms of piracy from your organization. We will examine two approaches to reducing risk; 1. The fast track to compliance for those organizations that would like to act quickly, and 2. A long-term solution that your organization should consider putting into place to accomplish the greatest effectiveness.

The Fast Track to Compliance.

1. Collect Proofs of Ownership

- Purchase Orders
- Paid Invoices
- Receipts for Purchase
- Original License Certificates

The “proofs of ownership” list is arranged in order of the potentially easiest items to locate and in reverse order of the most acceptable proof. That is not to say that purchase orders are not acceptable. They are often the most reliable, and most accurate, proof you will be able to locate. Auditors generally will prefer original license certificates over all other forms, but will usually accept anything on the list.

The most important thing to keep in mind in step one is that the list can be divided into two types of “ownership proof” and only one or the other is acceptable in a compliance audit. The first three items represent different types of “receipts” while the fourth is a “certificate of ownership”. You may mix the first three receipts as long as you can demonstrate that there is no overlap. But you may not mix receipts with license certificates.

Serial numbers are not proofs of ownership. They are useful to identify copies of software and their source and they are helpful when purchasing upgrades. But auditors will not accept the existence of serial numbers as proof of ownership. Additionally, original media (CD's, diskettes, and documentation) is less useful in today's world of multiple license packs and is generally unreliable in counting numbers of licenses.

2. Audit Installed Software

- Systematically Inspect Every
 - Desktop
 - Portable
 - Server
 - Home computer (optional)

Steps one and two can be reversed or done simultaneously. Both must be completed prior to reconciling and proving license ownership in step three. You will need an exhaustive list of all copies of software and their version numbers installed on all computers in your organization. Later we will discuss tools that

you can use for this task. Once you have completed steps one and two you are ready to discover how much of your organization's installed software is legally licensed.

3. Reconcile Audit & Proof of Ownership

- Product Names
- Version Numbers
- Types of Licenses (Single-user, Concurrent use, other restrictions)
- Serial Numbers

Compare the details in list three from your audit list and ownership proofs list for matches. The goal of step three is to discover any software in use on your site that cannot be traced back to its license. With each such discovery you then make the decision of whether to buy a license or delete the software. That's it in a nutshell – easy to describe, extremely difficult to accomplish – unless you have automated auditing and usage management tools in place (more on that subject later).

A Long-term Solution.

For a more long-term solution, add the following two steps to the first three above.

4. Establish Corporate Culture

- Publish Corporate Policy
- Have Employees Sign It
- Centralize Purchases
- Store Original License Certificates, Purchase Orders, Invoices, Receipts, Registration Cards
- Prevent or Detect Employee-Software Installs

There is nothing that can replace the value of well-designed and active anti-piracy education among the staff and students in your organization. Their understanding of the pitfalls and solutions will go a long way toward reducing risk within your organization. Add to that the organizational discipline of recording ownership as purchases occur, and you will create the important foundational basis upon which your company can build to effectively manage ongoing usage.

5. Manage Ongoing Usage

- Determine Ownership (department, division, or corporate organization)
- Manage Correctly by Type of License
- Who Should Have Access to Each Product?
- Track Computer Obsolescence and Stop Buying Software
- Identify Waste, Reclaim & Redistribute
- Predict Needs and Purchase Accordingly

Before you can effectively manage software usage to comply with your software licenses you must first know who owns the licenses. You must determine whether licenses have been purchased for use anywhere within your organization or only for use within specific departments, divisions, or regional areas of your company.

Next, you must understand what type of licenses your organization owns. Site licenses (licenses that can be installed anywhere within your organization) are the easiest to manage. However, unless you use great diligence to determine true usage they can cause the hidden problem of making it difficult for you to determine exactly how many units you should purchase. Concurrent-use licenses (licenses that can be shared by multiple users) are also convenient but they are the hardest to convince publishers to offer. Single-user licenses (licenses which must be locked to specific computers) are often the most expensive IT asset your organization owns and can create the biggest legal risk if not properly managed.

In the next section we will discuss how to effectively manage all of the major types of software licenses to reduce legal risk, lower ownership costs, and soften the fears and resulting resistance of software publishers to offer licenses that are truly useful to your organization.

How Can We Effectively Manage Ongoing Software Usage?

It is easy to understand, from the material we have covered so far, that effective management of a multitude of software programs within a diverse, and ever-changing, user community can be a complex task. The Sassafras Software solution first takes steps to simplify this daunting task by breaking down software management into four essential elements: computers, people, software, licenses.

The Sassafras KeyAuditor provides essential first steps through a unique auto-discovery process that identifies and locates installed software and reports important details about computer hardware. The Sassafras KeyServer takes the management process to the next step with flexible software license definitions that cover the full range of today's most common software licenses.

The final step of identifying end-users and authenticating them to use approved software accomplishes several important efficiencies. It closes the gap to potential software piracy. It creates a supported working environment where employees can gain legal access to software to complete their work effectively. And it helps organizations to achieve high levels of efficiency in the use of their software budgets.

Unresolved Questions - discussion points for buyers and sellers.

Much of the controversy and debate surrounding software-licensing stems from the disparate interests of corporate and educational end-users on one side and software publishers and resellers on the other. There are numerous unresolved questions that continue to linger in the software industry. We believe that the effective use of present-day and emerging software usage management technologies can produce inspired solutions to address the concerns and protect the interests of all parties.

Many questions have been resolved in the decade-plus since Sassafras Software pioneered the development of desktop license management technology in the late 1980's. Some questions that continue to linger are: Does each copy of an application found on each computer drive – whether the machine is currently in use or in storage – count? Does each have to be licensed? What about dormant software that is installed but unused on a computer that is in regular use? If a software program has not been launched for a considerable length of time (months or years) does it still need to be validated by a license?

Sassafras Software has devoted more than a decade of research and development to provide the currently available auditing and management tool chest found in KeyServer and KeyAuditor. We believe that through proper understanding, configuration, and management, the tools in our present day solutions will resolve each of the questions above. Please contact us to discuss these solutions in depth.

At Sassafras Software, we are always interested in addressing end-user and publisher's questions. We are also open to collaborative efforts with other industry leaders that will improve the environment of software licensing. If you have questions, or ideas for collaboration, please contact:

John Tomeny <johnt@sassafras.com>
Sassafras Software Inc.
PO Box 150
Hanover, NH 03755
603-643-3351