



Software Management Guide

*-a guide designed to assist you in effective
software management*

Software® Information Industry Association

1730 M Street NW

Suite 700

Washington, DC 20036

+1 (202) 452-1600

www.siiia.net

Dear Software Professional:

The SIIA¹ Software Management Guide was produced for one simple reason--you told us you needed it. As the SIIA travels the world spreading the word the legal use of software, we continually receive requests from auditors, internal auditors, MIS managers and software managers for a comprehensive, yet understandable guide to managing software as a strategic asset. This Guide approaches software asset management in a manner similar to the way in which auditors approach the management of other corporate assets.

This Guide was designed to educate software professionals about the legal and managerial issues surrounding compliance with software license agreements, software metering, and software asset management.

This guide contains four main sections. They are:

Section 1: The Copyright Law and Software License Agreements

This section of the guide is designed to give an overview of what the current copyright law is, and how it relates to software licensing issues.

Section 2: The SPA Eight Point Program for Ensuring Software Compliance

This overview helps you focus on the key items to promote compliance within your organization.

Section 3: Internal Controls Analysis and Questionnaire*

Before undertaking an audit, an assessment must be made of the organization's system of internal controls. This section provides the questions an auditor must ask to understand the general control environment, as well as the specifics of purchasing, backup and security procedures.

*NOTE: This section is available as an Adobe Acrobat (.pdf) file located at: <http://www.sii.net/piracy/pubs/smg4.1sec3.pdf>. It is not contained in this manual, however, it is integral to completion of a successful software audit.

Section 4: The Software Audit Program

This program sets forth procedures for auditing your firm's compliance with its software license agreements. It includes a step by step system for auditing all the personal computers in your organization, as well as a sample Software Audit Report and Management Letter.

¹ Note: The SIIA was formed on January 1, 1999, as a result of a merger between the Software Publishers Association (SPA) and the Information Industry Association (IIA). SIIA is the principal trade association of the software code and information content industry. SIIA represents 1,200 high-tech companies that develop and market software and electronic content for business, education, consumers, the Internet and entertainment.

Section 1:

Overview: The issues and the problem.

The SPA anti-piracy division of SIIA has been proactively assisting companies in getting legal, and staying legal since 1984. The guide is intended not only for business environments, but also for government, educational institutions and non-profit entities. While the following wording is geared to businesses, other groups can use it by simply incorporating the correct wording applicable to their environment. Use it freely and copy the forms and policy statements that may be helpful.

Every organization, regardless of type, has its own set of procedures that affect everything from personnel to procurement. These procedures ensure a smoothly functioning organization in which administrative matters do not impede the organization's mission. Organizations work best when employees understand and follow established administrative procedures. One guiding consideration for this publication is that its content be practical and flexible. Most importantly this guide is meant to be just that, a guide. Please make adjustments and additions so the various pieces contained herein fit your particular environment.

SIIA encourages you to adapt any or all of this guide to fit your needs. Additional information and resources are available at www.spa.org/piracy or www.sii.net/piracy.

Why worry about software licensing?

In recent years, the issue of software licensing and software piracy has come to the attention of computer users nationwide, often with staggering results. Organizations that saw no problem with copying software for employee use have been hit with stiff fines and other penalties for the mismanagement of the software installed on their workstations.

We are the only industry that empowers every user to become a manufacturing subsidiary.

*-Ken Wasch, president
SIIA*

A lax attitude toward software use is often due to the lack of an effective software management policy, employee education, and active support from upper management within the organizational environment.

Unfortunately, there are many people who either ignorantly or deliberately jeopardize that growth. Whenever you use a piece of software that is unlicensed, you are depriving the software companies of their earnings. More importantly, you are depriving the creative teams who have developed the software (*e.g., programmers, writers, graphic artists, etc.*) of the compensation for the thousands of hours they have spent working on a particular program.

Many computer users have found themselves caught in the piracy trap, unaware that they were doing anything illegal. To avoid such unpleasant surprises, it may be helpful to know the five basic ways a person can pirate software:

1. **Softlifting** -- Purchasing a single licensed copy of the software and loading it on several machines, contrary to the terms of the license agreement. This

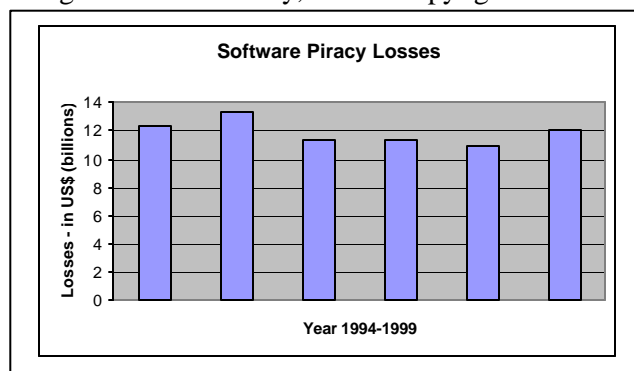
includes sharing software with friends and co-workers and installing software on home/laptop computers if not allowed by the license.

2. **Internet** – Uploading (or downloading) commercial software (*i.e., software that is not freeware or public domain*) on an online service or the Internet for anyone to copy or copying commercial software from any of these services.
3. **Hard-disk loading** -- Selling computers preloaded with illegal copies of software. If you buy or rent computers with preloaded software, your purchase documentation and contract with the vendor should specify which software is preloaded and that these are legal, licensed copies.
4. **Renting** -- Renting software for temporary use, like you would a video. Software rental was made illegal in the United States by the Software Rental Amendments Act of 1990 and in Canada by a 1993 amendment to the Copyright Act.
5. **Counterfeiting** -- Duplicating and selling unauthorized copies of software in such a manner as to try to pass off the illegal copy as if it were a legitimate copy produced or authorized by the publisher.
6. **OEM Piracy/Unbundling** – Some software, known as OEM (original equipment manufacturer) software, is only distributed when sold with specified accompanying hardware. When these programs are copied and sold separately from the hardware, this is a violation of the contract with the publisher. Similarly, the term “unbundling” refers to the act of selling separately software that is legally sold only when bundled with another package. Software programs that are marked “not for resale” are often bundled applications.

As you can see from the various types of piracy described above, it is easy to become an "accidental pirate." This is part of the reason piracy has become so costly to the software industry.

According to SIIA, in 1999, domestic piracy of PC business software applications cost software developers US\$3.1 billion in the United States. Put simply, this loss means that one of every four copies of business application software is illegal. Internationally, where copyright law is less frequently enforced, the losses are even greater. The software industry estimates that it may be losing more than US\$12 billion worldwide to piracy.

Anyone who acquires legal software has the right to load it onto a single computer, and to make one copy for "backup" or "archival purposes." That is the **only** copy you are authorized to make according to the terms of the U.S. Copyright Act. Individual software license agreements frequently grant users more rights than they are allowed under the U.S. Copyright Act and may allow for more than a single archival



copy, and should be read and understood before using the software. Making additional copies or loading the software onto more than one machine or on a network may violate copyright law and be considered piracy. What follows is a definition of the US Copyright Laws, followed by a discussion of the licenses accompanying the software products.

What is the Copyright Law?

THE U.S. COPYRIGHT ACT

The US Copyright Act, found at Title 17 of the US Code, automatically protects software from the moment of its creation and fixation in tangible form. Except for the rights to (i) copy the software onto a single computer and (ii) make "*another copy for archival purposes only*," which are provided in the act (Section 117), any other use without the permission of the copyright owner is prohibited.

The US Copyright Act also gives certain exclusive rights to the copyright owner, namely to "*reproduce the copyrighted work*" and "*to distribute copies...of the copyrighted work*" (Section 106). The exclusive right of reproduction includes making copies of computer programs in any format. These formats include magnetic and optical disk, computer memory for personal computers, and networks. The exclusive right of distribution includes any sale, lease, rental, or transfer of such copies. The right of distribution also includes the exclusive right to offer to transfer copies, regardless of whether payment is received. Moreover, it embodies distribution by any means, including electronic distributions via the Internet and other networks.

The copyright law encourages legal software use. It is designed to create deterrence from making unlawful copies of software and incentive for lawful use.

The US Copyright Act also states that "*anyone who violates any of the exclusive rights of the copyright owner...is an infringer of the copyright*" (Section 501). This section proceeds to list several penalties for this infringement, including liability for damages suffered by the copyright owner plus any profits of the infringer that are attributable to the copying, or statutory damages of up to US\$150,000 for each work infringed. In addition, the copyright owner can recover attorney's fees from the infringer. The unauthorized copying or distribution of software is a federal crime if done "*willfully and for purposes of commercial advantage or private financial gain*." This includes the receipt of anything of value, like bartered software, or willfully making multiple copies with a value of more than \$1000. Criminal penalties include fines of as much as US\$250,000 and jail terms of up to five years.

In simpler terms, if you wish to remain free of legal entanglements, you should be sure you have the legal right to copy or distribute copies of a piece of software before doing so.

Reasons for Following the Terms of Software Licenses

While computer software is a new form of intellectual property, it is covered under the same provisions of copyright law that protect music, books and film from unauthorized distribution. Like the more traditional media, infringement of copyright law involving computer software carries with it stiff penalties.

All software comes with a license that specifically states the terms and conditions under which the software may be legally used. Licenses vary from program to program, and may authorize as few as one computer or user to use the software, or as many as several hundred network users to share the application through the system. It is important to read and understand the license agreement accompanying the program to ensure that you have sufficient legal copies of the software for your organization's needs. Users of software programs need to have a specific contact within their organization for their software licensing questions. Appointment of a software manager, or possibly a representative in the company's legal department should be made known to all employees so that specific questions can be asked of the software license in question.

The most fundamental aspect of a successful software policy, outside of the policy itself, is the actual software audit. If a software audit determines that your organization is using unauthorized (*i.e., pirated*) copies of software, the organization may face not only a civil suit for damages and any profits attributable to the pirated software, but corporate officers and individual employees may be charged with criminal liability as well. This may also include fines and jail terms. Taking steps to prevent the use of illegal software and ensure compliance with copyright law can save your organization the expense and embarrassment of this kind of legal action.

The Consequences of Not Managing Software Licenses

Risks of Illegal Software:

- ❑ Fines of up to \$150,000 per infringed title.
- ❑ Lack of product support
- ❑ Blemished reputation – “hey, you were the one’s busted”
- ❑ Possible criminal charges against directors/managers
- ❑ No product warranties, possible virus penetration

SPA Anti-Piracy, a division of SIIA, was organized to promote, protect and provide information to the software industry. Since 1988, SIIA has been actively enforcing copyrights on behalf of its 1200 member companies. In addition to SIIA, there are several software companies who actively pursue infringement actions on their own.

SIIA continues to be aggressive because the losses suffered through piracy directly affect the profitability of the software industry. In the past four years, SPA has brought thousands of cases against end users in the United States and abroad. Settlements have been as high as US\$500,000 in a single case.

In a very real sense, the piracy of software, both domestic and foreign, adversely affects the world economy by diverting money that stimulates further product development. Piracy particularly affects the United States, which currently provides approximately 80 percent of the world's software.

Software piracy is found in almost every type of business and SIIA has brought actions against all types of organizations: Fortune 500 corporations; hospitals; nonprofit institutions; schools; and small businesses with as few as 10 PCs.

For more information on the SIIA anti-piracy program, please go to:

<http://www.spa.org/piracy/> or <http://www.siia.net/piracy>.

Section 2: SIIA's Eight Point Program for Ensuring Software Compliance

Introduction

This eight point program outlines a number of areas that must be integrated to provide a comprehensive approach to software management within the organization. More detailed information follows.

- 1. Appoint a software manager.*
- 2. Implement a software policy.*
- 3. Establish procedures for acquiring, registering, storing, utilizing, and backing up software.*
- 4. Establish and maintain a software log.*
- 5. Conduct periodic audits.*
- 6. Establish an employee education program.*
- 7. Maintain a library of software licenses and registration materials.*
- 8. Enjoy the benefits of software license compliance.*

Each of these points will be discussed in turn.

1. APPOINT A SOFTWARE MANAGER

The manager is responsible for implementing all aspects of software policy, maintenance of detailed records and supervision of compliance. The importance of assigning a specific person to this task must be emphasized. To ensure a comprehensive, uniformly administered program, employees should have access to a single individual knowledgeable about all aspects of the organization's software policy. In addition to effective coordination, assigning a person to this role sends a strong signal about the organization's commitment to software license compliance to its employees and vendors. In larger organizations the software manager should be someone in the MIS or Audit/Administrative functions.

2. IMPLEMENT A SOFTWARE POLICY

The organization's software policy should be developed, maintained and signed annually by all employees (*and by new employees at the time of hire*). It should be made a condition of employment and should be documented as such in employee handbooks and organization hiring policies. For effective implementation, it is critical to develop an education program to explain your

software policy to all employees. Your program's goal should be to restate your management's commitment to original software use in compliance with all license agreements. Your educational program should emphasize that illegal copying of software is a serious offense, contrary to both the law and your organization's policy. The educational program should discuss all aspects of the policy statement including: anti-piracy statement; acquisition, utilization, and auditing procedures; backup, storage, security, and maintenance procedures; disaster recovery procedures; training and support activities; documentation and software compliance; planning and budget procedures; home computers; and policies regarding installment of non-organization owned software. You should also specify the organization's penalties for employees who do not comply with these policies.

3. ESTABLISH PROCEDURES FOR ACQUIRING AND REGISTERING SOFTWARE

a. Needs Assessment. Software purchasing decisions should be assessed like any other organization investment. The organization defines its software requirements, supervisors approve the requirements, and software packages are evaluated to determine which is best for the organization. This process should be as prompt and efficient as possible so as to not create the situation where an employee is "forced" to make a copy of a software program to complete a specific task.

b. Planning and Budgeting. Just like hardware acquisitions, software purchases should be budgeted. When planning hardware purchases, budget for new software for the new CPUs and new software needed for existing equipment. Providing for only computer hardware purchases encourages illegal software copying. Software purchases can equal 50 percent or more of the cost of the computer. Because it is a significant expense, and because software is a critical component of the information processing function, it should be budgeted along with other aspects of information processing. To obtain the maximum value from your software assets, you should also budget for employee training. The key to developing a realistic budget is to effectively implement the first step -- the evaluation of the organization's requirements for software, hardware, training and maintenance.

c. Purchasing. It is essential that the purchasing of software be a standard procedure just like the acquisition of other critical assets. All software purchases should proceed through the organization's normal purchasing channels, which in most organizations requires a purchase order and supervisor or management approval. Even though some software packages may be inexpensive, software should not be purchased through employee expense reports, travel reports or from department petty cash, because it is then difficult to track purchases for budgeting and other purposes.

d. Registration. The software manager should complete registration cards for all software as it is purchased and delivered, or in the case of online software purchases, the software manager should complete the online registration form at the software publisher's website. Promptly completing this process ensures that the organization will receive product support and timely product announcements. Registration of all organization software should be in a standard format, such as organization name and department. Therefore, when individuals leave, the software stays with the organization and notifications of upgrades will be sent to the organization. Also the publisher will have a record of the purchase that duplicates your purchase order and receipts. A Software Log (*which will be discussed more fully below*) may prove helpful in tracking software acquisitions and registration.

e. Storage and Security. After installing the program on the hard disk, the software manager should keep the original software in a separate, secured, storage area. By ensuring secure storage, the risk of software theft and unauthorized duplication of software is minimized. Original software should be stored so that they are not subject to damage by environmental factors such as heat, fire, and water. This process should be supervised by the software manager.

f. Documentation. Original manuals, tutorials and other user-oriented documentation should reside with the software user. This encourages employees to purchase legitimate software. If you work in a network environment, you may opt not to distribute a manual to each user. In that case, be sure to designate a resource person to respond to questions.

g. Home Computers and/or Laptops. If your employees are like most, it is not unusual for them to take work home or bring personal software to the office. This is another area of potential risk. Generally, employees should not be permitted to bring software from home and load it on organization computers because of the risk this poses from viruses unwittingly brought in on the employee's software. An organization's computers are important assets and risks to assets should be minimized. To ensure that all software used in an organization is both legal and virus-free, software should be purchased and installed through the organization's established software acquisition process only.

4. ESTABLISH AND MAINTAIN A SOFTWARE LOG

The software manager should maintain a log of all software purchased by the organization (*see sample, below*). The software log should note the location of each software package and the CPU on which the software is installed. If your organization does not yet have an organization-wide inventory, the best way to obtain one is to conduct an audit of your computer resources. After ensuring that all software has been legally purchased, the audit results can serve as the basis for the software log. The software manager then can update the log database with each new software acquisition. The log must contain the following:

The date and source of software acquisition, including details of the site license, volume discount or network version terms, and software serial number (if appropriate).

- The location of installation, as well as the serial number of the hardware on which each copy of software is installed.
- The name of the authorized user.
- The existence, location and number of original disks.
- Copy of the completed registration card, or electronic equivalent if registration is completed online at the publisher's website.

Helpful Hint: If you have standardized your software purchases through one reseller, or a small handful, resellers can provide proof of license reports to you indicating what software you have lawfully acquired from them. Alternatively, some software management programs will also assist you in tracking your software assets.

The software manager should also maintain copies of the original license agreement and any other documents showing legitimate acquisition of software so as to have available for future reference. This should be filed with the purchasing documentation mentioned above.

Licensed software often falls below organization guidelines for capitalization as a fixed asset. Then they are not tracked as part of a fixed asset system, and the software can often be lost or invisible to organization records. The investment in software, as well as copyright compliance issues, make the software log an essential management tool. The software log should, of course, be computer-based and must be backed up.

SOFTWARE LOG

Product & Version	Publisher	Software Serial #	Purchase Date	User Name	User Location	Hardware Serial #	Comments*

* Comments should include location of backup copies.

5. CONDUCT PERIODIC AUDITS

An audit of your software resources will provide several benefits to your organization. First and foremost, the audit allows you to determine compliance with the various aspects of your organization's software policy. To be comprehensive, it should include, but not be limited to a review of the following:

Software audits are important for more than simply determining what software is installed. They also assist you in determining use, potential over-licensing of product, and lastly any shortfall.

- the organization's software education program
- the software log and license agreements

- the organization's software budget
- the actual software found residing on the organization's computers
 - the software purchase records

The audit may be conducted by organization employees, such as internal audit personnel, or outside persons, such as a CPA or a consulting firm. The auditors must have adequate training to conduct a comprehensive examination of your software compliance. To maintain your policy of software excellence, audits should be conducted regularly (*at least annually*). To conserve resources, you may find it useful to combine the software audit with a hardware audit and a virus check. *SIIA's anti-piracy site maintains a list of audit tools that may be appropriate for your organization.*

6. ESTABLISH AN EMPLOYEE EDUCATION PROGRAM

To ensure that your software compliance program is ultimately successful, it should be supported by an organization-wide education program -- one that targets its message to all employees from senior managers to support staff. The educational program should have the following components:

- Explain the software code of ethics and the organization's policy.
- Enlighten employees about software piracy and why it is a problem. All new employees should take the education course as part of their employee orientation program.
- Explain the hidden costs of illegal software, such as the prospect for fines and possible sanctions against the company and/or employee.

These goals can be met in a variety of ways and can be combined with education programs relating to other IS issues such as backup of user data, security policies, training and support programs, etc. To assist you, you may wish to use copies of SPA's various anti-piracy materials.

7. MAINTAIN A LIBRARY OF SOFTWARE LICENSES

License agreements for the software products you purchase will not be uniform. Yet it is important for your software manager to compare and understand these agreements, because by using the software product your organization has agreed to be bound by the terms of the product's license. The software manager should not only become familiar with the license agreements of the software products used by the organization, but should also be responsible for maintaining a library of product licenses. Employees should be provided with copies of each applicable license agreement, or have access to them. Alternatively, the software manager may provide a summary of the agreements for the most widely used products in the organization. In cases in which a license agreement does not exist, such as custom software or software developed as in-house software, an "*internal license agreement*" should be drafted explaining organization policies regarding the use of the software.

8. ENJOY THE BENEFITS OF SOFTWARE LICENSE COMPLIANCE

Why should a computer user be concerned with software compliance? It is the law, but there are also valuable benefits for becoming software legal. With original computer software, users receive full documentation, technical support and upgrade notifications. The user will also be investing in the quality assurance and reliability of the product. Legal compliance means that the business relationship does not end when the buyer walks out of the store. The organization will also enjoy the efficiencies of fully operational and productive employees and computer systems and virus protection.

These goals can be met in a variety of ways and can be combined with education programs relating to other IS issues such as back up of user data, security policies, training and support programs, etc. The following materials are available from SIIA.

Useful tools available from SIIA to further assist you in this important effort:

- **It Could Have Been So Easy.** a video educating employees and management about the risks of copyright infringement. It's an excellent employee training tool for organizations of all sizes.
- **SPAudit and/or KeyAudit.** Software programs published by WRQ (WRQ Express Inventory, SPA Edition) and Sassafra KeyAudit that assist you in performing a software audit by determining what programs reside on the organization's hard disks.
- **Software Use and the Law** a brochure that details how the copyright law applies to software. Detailed information is provided for management and IS professionals.
- **The Better Business Bureau (BBB) brochure Computer Software Piracy.** This brochure offers dependable tips and helpful information .



SPA Certified Software Manager (CSM) course is a one day event designed to help organizations manage their PC assets effectively to ensure they are using software legally, to optimum advantage and at lowest cost. For more information, please go to:
<http://www.sii.net/piracy/seminars/csm.asp>.

- **Suggested Policies and Procedures** – standard templates available from www.spa.org/piracy or www.sii.net/piracy. These documents, reproduced below, allow you to utilize language informing your employees of their responsibilities in respect to the use of software.

These and other materials are easily accessed by going to:

www.spa.org/piracy, or www.sii.net/piracy.

Software Code of Ethics

Employee Software Usage Guidelines

Software will be used only in accordance with its license agreement. Unless otherwise provided in the license, any duplication of copyrighted software, except for backup and archival purposes by software manager or designated department, is a violation of copyright law. In addition to violating copyright law, unauthorized duplication of software is contrary to [organization's] standards of conduct. The following points are to be followed to comply with software license agreements:

1. All users must use all software in accordance with its license agreements and the [organization's] software policy. All users acknowledge that they do not own this software or its related documentation, and unless expressly authorized by the software publisher, may not make additional copies except for archival purposes.
2. [Organization] will not tolerate the use of any unauthorized copies of software or fonts in our organization. Any person illegally reproducing software can be subject to civil and criminal penalties including fines and imprisonment. All users must not condone illegal copying of software under any circumstances and anyone who makes, uses, or otherwise acquires unauthorized software will be appropriately disciplined.
3. No user will give software or fonts to any outsiders including clients, customers, and others. Under no circumstances will software be used within [organization] that has been brought in from any unauthorized location under [organization's] policy, including, but not limited to, the Internet, the home, friends and colleagues.
4. Any user who determines that there may be a misuse of software within the organization will notify the Certified Software Manager, department manager, or legal counsel.
5. All software used by the organization on organization-owned computers will be purchased through appropriate procedures.

I have read [organization's] software code of ethics. I am fully aware of our software compliance policies and agree to abide by them. I understand that violation of any above policies may result in my termination.

EMPLOYEE SIGNATURE

DATE

You are permitted to reproduce and modify this document so long as attribution is given to SPA.

Organization Software Usage Guidelines

1. General Statement of Policy. It is the policy of [organization] to respect all computer software copyrights and to adhere to the terms of all software licenses to which [organization] is a party. [Organization] will take all steps necessary to prohibit users from duplicating any licensed software or related documentation for use either on [organization] premises or elsewhere unless [organization] is expressly authorized to do so by agreement with the licensor. Unauthorized duplication of software may subject users and/or [organization] to both civil and criminal penalties under the United States Copyright Act. [Organization] must not permit any employee to use software in any manner inconsistent with the applicable license agreement, including giving or receiving software from others.

2. User Education. [Organization] must provide and require a software education program for all of its software users (to be crafted by the software manager). Upon completion of the education program, users are required to sign the [organization's] Employee Personal Computer Software Usage Guidelines. New users will be provided the same education program within 10 days of the commencement of their employment.

3. Budgeting for Software. When acquiring computer hardware, software and training, [organization] must budget accordingly to meet the costs at the time of acquisition. When acquiring software for computers, [organization] must charge the software to the department's budget for IT or an appropriate budget set aside for tracking software acquisition.

4. Acquisition of Software. All software acquired by [organization] must be through the [MIS, purchasing, or other appropriate] designated department. Software may not be acquired through user corporate credit cards, petty cash, travel or entertainment budgets. Software acquisition channels are restricted to ensure that [organization] has a complete record of all software that has been acquired for [organization] computers and can register, support, and upgrade such software accordingly. This must include software that may be downloaded, used via an Application Service Provider (ASP) or acquired from the Internet.

5. Registration of Software. When [organization] receives the software, the designated department (MIS, purchasing, etc.) must receive the software first to complete registration and inventory requirements before installation. In the event the software is shrink-wrapped, the designated department is responsible for completing the registration card and returning it to the software publisher. Software must be registered in the name of [organization] and department in which it will be used. Due to personnel turnover, software will never be registered in the name of the individual user. The designated department maintains a register of all [organization's] software and will keep a library of software licenses. The register must contain: a) the title and publisher of the software; b) the date and source of software acquisition; c) the location of each installation as well as the serial number of the hardware on which each copy of the software is installed; d) the existence and location of back-up copies; and e) the software product's serial number or other identifying information.

6. Installation of Software. After the registration requirements above have been met, the software will be installed by the software manager. Once installed, the original media will be kept in a safe storage area maintained by the designated department. User manuals, if provided, will either reside with the user or reside with the software manager.

7. Home Computers. [Organization's] computers are organization-owned assets and must

be kept both software legal and virus free. Only software purchased through the procedures outlined above may be used on [organization's] machines. Users are not permitted to bring software from home and load it onto [organization's] computers. Generally, organization-owned software cannot be taken home and loaded on a user's home computer if it also resides on [organization's] computer. If a user is to use software at home, [organization] will acquire a separate package and record it as an organization-owned asset in the software register. However, some software companies provide in their license agreements that home use is permitted under certain circumstances. If a user needs to use software at home, he/she should consult with the software manager to determine if appropriate licenses permit home use.

8. Shareware. Shareware software is copyrighted software that is distributed via the Internet. It is the policy of [organization] to pay shareware authors the fee they specify for use of their products. Under this policy, acquisition and registration of shareware products will be handled the same way as for commercial software products.

9. Quarterly Audits. The software manager or designated department will conduct a quarterly audit of all [organization's] PCs and servers, including portables, to ensure that [organization] is in compliance with all software licenses. Surprise audits may be conducted as well. Audits will be conducted using an auditing software product. Also, during the quarterly audit, [organization] will search for computer viruses and eliminate any that are found. The full cooperation of all users is required during audits.

10. Penalties and Reprimands. According to the US Copyright Act, illegal reproduction of software is subject to civil damages of as much as US\$150,000 per title infringed, and criminal penalties, including fines of as much as US\$250,000 per title infringed and imprisonment of up to five years. An [organization] user who makes, acquires, or uses unauthorized copies of software will be disciplined as appropriate under the circumstances. Such discipline may include termination of employment. [Organization] does not condone the illegal duplication of software and will not tolerate it.

I have read [organization's] anti-piracy statement and agree to bind the [organization] accordingly. I understand that violation of any above policies may result in both civil liability and criminal penalties for the [organization] and/or its employees.

SIGNATURE

TITLE

DATE

You are permitted to reproduce and modify this document so long as attribution is given to SPA.

Section 4: Software Audit Program

Introduction

This audit program provides you with specific audit steps to determine compliance with your organization's software license policy and the license agreements of your software vendors. As with any audit approach, there are numerous audit judgments which must be made to properly implement the audit's components.

Software license compliance is not only a legal responsibility, but failure to comply may impact an organization financially, since an organization may be held liable for unlicensed copies of software. The objective of an audit is to determine your organization's compliance with software license agreements.

Part 1: Internal Controls Questionnaire Summary

PURPOSE

To summarize the information obtained from the Internal Controls Questionnaire.

- A. Management interviews: Complete the Internal Controls Questionnaire by interviewing management and other personnel responsible for these controls.
- B. Walk through: Perform a walk through of the organization's software control system to ascertain that it is functioning as described.
- C. Summary memo: Write a memo summarizing the strengths and weaknesses of the organization's system. Evaluate each of the controls as weak, adequate, or excellent in preventing unlicensed software copying. Plan further audit steps accordingly.

Part 2: Inventory of Software Resources

PURPOSE

To determine the quantity of each software product in use in the organization.

- A. Determine the quantity of purchased software using non-purchasing data or documentation. In preparation, have all users gather as many of the following as possible for their personal computers:
 - original system diskettes and backup copies
 - original software documentation and manuals
 - original license agreement
 - original vendor registration card
 - purchase orders, invoices, or canceled checks

B. Obtain a list of all personal computers by location and serial number. Include network servers if applicable.

1. Test the list of personal computers:

- Ensure items on list exist at proper locations (*trace from list to location*).
- Ensure that items at each location appear on the list (*trace from location to list*).

2. Perform a count of all software on the personal computers using SPAudit or another software audit program.

- If using SPAudit, make sure to add any software products that are not included on the list of products for which SPAudit searches. Read the user documentation for products used to conduct the audit in lieu of SPAudit.
- List the software on each machine by the personal computer's serial number, employee number, telephone extension, or employee name.
- Summarize the software count by product and version number (*e.g., Norton Utilities version 8.0*).
- Use the Software Audit Worksheet to record:
 - a) Personal computer serial number and location
 - b) Software title, publisher, version, and identification number
 - c) License support documentation found including: system diskettes; software documentation and manuals; license agreements with serial numbers; registration cards; or other proof of purchase.
- Print out a hard disk directory of all *.EXE and *.COM files to check if there are additional software products on the PC that were not identified by SPAudit.

SIIA's anti-piracy program, done on behalf of our 1200 member companies, can conduct the following actions:

- 1. Cease and desist notices;*
- 2. Cooperative Audits; and*
- 3. Litigation.*

SIIA bases its decision on the sources information, member input and our decade of experience in doing this type of work

Part 3: Match Purchasing Documentation with Inventory

PURPOSE

To establish the quantity of software products actually purchased, you will next compare your results from the inventory of resources with purchase records.

A. In preparation:

- Have organization personnel find all purchase records related to software products (*invoices, purchase orders, email confirmation of online purchases, check registers, canceled checks, general ledger account activity*). *You may also want to consider contacting your software vendor/reseller as they may be able to assist you in this effort.*
- Separate purchase records by product/version.
- Summarize purchasing data by product, version and serial number and post to software audit worksheet.

- B. Review the fixed asset register to locate additional software that has been capitalized with system hardware.
- C. Review department budgets for current and prior years to ascertain plans to acquire legal software.
- D. Check the appropriate budget to determine if budgeted software was actually acquired.

**Part 4:
Calculate License Violations**

PURPOSE

To determine the dollar amount by which your organization is out of compliance with applicable licenses. That amount, labeled "violation value," indicates the cost to purchase additional software licenses to ensure full compliance.

- A. Using the Software Audit Worksheet Summary, calculate the number of software license violations by product and version.
- B. Calculate the dollar value of violation by multiplying the number of violations by the list price of the software.
- C. Total all violations to determine exposure.

How are cases generally settled?

After determining the illegal software, the company must:

- 1. Destroy that unauthorized software;*
- 2. Obtain legal software to replace that which is needed;*
- 3. Pay a fine equal to a multiple of the value of the infringing software found and legal fee's*
- 4. Commit to using legal software in the future.*

- D. Destroy all unlicensed software and repurchase authorized copies. Maintain a record of the software destroyed and the computers on which such copies were removed.

**Part 5:
Additional Procedures**

PURPOSE

To determine any other possible violations not found during the course of the audit.

- A. Discuss software purchases with financial auditors and/or legal counsel to determine if they are aware of any aberrations.
- B. Make sure there is a licensed copy of the operating system licensed for each computer.

Part 6: Audit Report and Management Letter

PURPOSE

To inform management of the results of the audit and to make recommendations for future controls.

A. Prepare a Software Audit Report to management explaining the procedures performed and their results. Specify the number of copies found, licensed, and the shortfall.

B. Prepare a separate Management Letter with suggestions to management to correct copyright infringement exposure and to improve controls over software procurement, use and reproduction.

Software Audit Report and Management Letter

The audit report is your tool to communicate to management the procedures performed and the results of those procedures.

For CPAs, this engagement qualifies as the performance of *"agreed-upon procedures."* Accordingly, the first paragraph of your report has to be in compliance with the standards established by the AICPA. Other auditors, such as internal auditors or consulting firms, need not have the *"agreed-upon procedures"* paragraph in their report.

The report should summarize both the procedures and results. Of course, only the significant items need to be included.

Following is an example of a report to management. It shows not only the basic format, but includes examples of specific items that you may want to include.

Sample Audit Report

Date

CEO

Organization

Address

Dear Mr./Ms.:

Pursuant to my responsibilities as software manager, I have supervised the completion of a personal computer software audit of [organization]. We have followed the procedures recommended by the Software Publishers Association. These procedures and our findings are summarized below.

PROCEDURE

1. We reviewed the software policy of the organization and its implementation and controls. This included responding to the questions in our software internal controls questionnaire, a copy of which is provided.
2. We also audited the organization's inventory of software resources including a list of all personal computers by location and serial number. Using SPAudit (*or a similar auditing product*), we obtained a list of all the software on the hard disk of each computer.
3. We matched purchasing documentation with the software inventory record we assembled. This included reviewing software purchase records such as invoices, purchase orders, check registers, canceled checks, manuals, diskettes, license agreements and registration cards.
4. We calculated the value of the license violations that we found.

FINDINGS

In the area of software policy and controls we found the organization owns a total of 345 legal copies of 5 applications from 5 vendors. Of those owned, 83 programs had no record of registering the software with the publisher. In addition, we identified 143 copies of software programs for which we had no corresponding purchase records and, therefore, appear to be illegal copies.

Of the 115 personal computers, we found 14 machines with software that had been brought from home by employees.

We found a number of employees with software on their machines for which they had received no formal training.

SOFTWARE LICENSE VIOLATIONS

The following is a summary of the software license violations which we found:

Product	Copies Found	Legal Copies	Shortfall
Norton Utilities	78	32	46
AutoCad R14	49	15	34
Microsoft Office	99	75	24
AutoCad 2000	32	30	2
Windows 2000	87	50	37

The total value of the software for which we did not have licenses (*the number of illegal copies times the suggested retail price*) was \$41,285.99.

We have already deleted all copies in excess of the number of legal copies and are now fully in compliance with applicable software licenses. We have also ordered legal software to replace the software that was destroyed.

While some departments had little or no illegal software, others had significant quantities. I therefore recommend that we institute a one-hour training program on the legal use of software and stricter software inventory controls, including semi-annual spot audits. The training program should be repeated weekly over the next few months to permit all employees to attend. All employees should sign a code of ethics statement upon completion of the training program. In addition, all new employees should be required to participate in the program within two weeks of their start date.

Sincerely,

[name]
Software Manager

M=Manual D=Diskettes L=License Agreement R=Registration Card w/serial #
I=Invoice C=Canceled Check

*Source: Software Publishers Association

I=Invoice C=Canceled Check

*Source: Software Publishers Association

Auditing a Network

The software audits of network environments can be considerably more complex than stand-alone PCs. This is particularly true where networks are linked to other networks.

There are some network utility software packages that can help count the number of actual users of a piece of software. This is important particularly where licenses are issued for concurrent users and you must determine how many users are using the software at any given period of time.

Following are some additional steps and ideas that may help you to audit in a network environment.

1. Determine the exact number of personal computers and/or terminals that are directly attached and have either file access or software access to this network.
2. Determine what software is installed on the server. Review the license, the invoice, the registration card, etc., for the number of licensed users allowed for each software application.
3. For each software package on the network determine:
 - a. The number of users of each software package. This is important for licenses based on users. Calculate if the company is in compliance or if the number of users exceeds the license, and note this to management.
 - b. If the software is licensed by LAN nodes, compare the number of licenses to the number of PCs on the network.
4. Using SPAudit or other software, determine software on local drives (physically attached disk drives).
5. Using SPAudit or other software, determine software on all remote drives in networks to which the user has access.
6. Use software other than SPAudit to determine the number of individuals who currently use the software at any given point in time.

Note: If software on network has been downloaded onto a local drive, the local drive copy is usually counted as a separate stand-alone copy for which a separate license is required. Check the specifics of the software license.

This document makes every attempt to make the job of software management an easier one. It is not meant to be the “end-all” cure. Instead, its design is to provide additional insight on some of the resources available, and have you also consider issues you may not have considered.

This document will be updated periodically. Since the nature of software use and licensing is evolving, so too will this document. Any comments to it should be directed to the address below.

Software Information Industry Association

1730 M Street NW

Suite 700

Washington, DC 20036

Phone: + 1(202) 452-1600

Fax: + 1 (202) 223-8756

www.siia.net/piracy or www.spa.org/piracy

Anti-Piracy Hotline (800) 388-7478 (U.S. & Canada)

The Software & Information Industry Association (SIIA) is the principal trade association of the software code and information content industry. SIIA represents more than 1,200 leading high-tech companies that develop and market software and electronic content for business, education, consumers and the Internet. Hundreds of these companies look to SPA Anti-Piracy, a division of SIIA, to protect their intellectual property rights around the world.

Version 4.1

