
The
Software
Alliance
BSA
Software
Asset
Management
Guide

WHY MANAGE SOFTWARE ASSETS

Introduction

IN TODAY'S ECONOMY, software is indispensable to every organization, large and small. Thanks to software, businesses are more efficient and workers are more productive.

In every sector of the global economy, organizations of all types rely on software to communicate, to make products, to offer services and to manage operations. However, keeping track of software assets can be a challenge, especially for large enterprises. More divisions, more teams, more projects mean more software — and mismanaging it can expose the organization to a slew of risks, from inefficiency to legal liability. To get the most out of software, it has to be managed well, just as any other valuable company asset. Poor software management robs companies of the full productivity and efficiency value of software, and therefore increases risk.

Effective software management combines the needs of an organization's IT assets with the needs of the company and of the individual. In both traditional and cloud environments, the practice of managing the lifecycle of software assets within an organization and remaining compliant with software license agreements is critical.

BSA | The Software Alliance stands ready to help businesses obtain benefits and avoid problems by implementing sound software asset management (SAM) practices. This overview covers the following topics to better understand the benefits and tools needed for implementation of a SAM program:

- The Benefits of Effective Software Management
- The Risks of Unauthorized Software Use
- How to Manage Software Properly
- Preventing Software Piracy in the Workplace
- Sample Corporate Software Policy
- Sample Memorandum to Employees
- Sample Software Needs Analysis Form

The Risks of Unauthorized Software Use

Unlicensed software can have costly consequences for your business.

Unlicensed software is more likely to fail as a result of an inability to update. It also is more prone to contain malware, rendering computers and their information useless. Expect no warranties or support for unlicensed software, leaving your company on its own to deal with failures.

There are legal consequences for unlicensed software as well, including stiff civil penalties and criminal prosecution. Software pirates increase costs to users of legitimate, authorized software and decrease the capital available to invest in research and development of new software.

Benefits

The Benefits of Effective Software Management:

Considering Software as a Valuable Asset Has Advantages

Software Asset Management (SAM) is the practice of managing the lifecycle of software assets within an organization. It is a set of managed processes and functional capabilities throughout the five stages of their lifecycle (planning, requisition, deployment, maintenance, and retirement). The two significant benefits of a SAM program are cost control and risk reduction.

Software can represent 25 percent of an organization's information technology budget. As a result, it makes fiscal sense to keep a close eye on what is spend to acquire software, to support and train staff to use it and to obtain the hardware, whether on premise or in the cloud, needed to make it work. A good SAM plan means a company acquires only the software that it needs, ensuring employees only use properly licensed software. Companies pay to upgrade only what's being used, and thus enjoy volume discounts by planning purchases and upgrades accordingly.

The key to cost control is budgeting for software as a separate expenditure line item. There are two benefits to this. First, software purchases and upgrades can be planned in an orderly way. With a separate software budget, needs can be anticipated, which avoids excessive spending or unexpected costs. Second, having a software budget enables purchases to be accurately tracked to easily spot unauthorized copies of software in an enterprise.

Purchasing only the authorized software needed, cuts down upgrade costs. Since you know what products are being used and in what quantity, only those copies where the new features will be of use will need to be upgrades. A coordinated upgrade policy ensures that an entire business keeps pace with industry standards and technology improvements.

Controlling software purchases and upgrades means savings on infrastructure and hardware as well. By providing software only to employees who need it, an enterprise avoids having to upgrade, add, or replace hardware or bandwidth for employees who don't need the capacity.

Planning software license acquisitions and upgrades can help employees anticipate changes during the year through notifications of new software installations and feature availability. The planning process also accounts for any training and support that will be needed as new software, services including cloud or employees are introduced. This results better prepared, more efficient and more productive employees.

Risks

The Risks of Unlicensed Software Use

Computer software is intellectual property (IP) owned by the entity that created it. Without the express permission of the manufacturer or publisher, it is illegal to install software, no matter how it is acquired. That permission almost always takes the form of a license from the publisher, which accompanies authorized copies of software. When software is purchased, the user is really acquiring a license to use the product. Rather than owning the software, an individual or enterprise acquire limited rights to use, reproduce, and distribute the program, according to the terms spelled out in the license agreement.

Typically, a licensed copy of a program can be installed and used on only one computer at a time, or to an authorized user as defined in the license agreement. Not complying with the terms of the license, for example, by installing the same copy of a single-user program on several computers or sharing a log-in credential to access cloud services where not permitted, is unauthorized. The publisher can take legal action against any individual or business who engages in these kinds of activities.

Software accessed remotely via the Internet, commonly called software as a service (SaaS), generally comes with multiple restrictions on use. In many cases, the restrictions are not negotiable given the nature of the SaaS contracts. Customers need to have proper controls in place to ensure compliance with all contractual requirements and limitations. Examples of these limitations may include prohibitions on use outside of a defined geography and restrictions on providing user access to non-employees, such as contractors.

A license isn't the only way software is protected. Copyright and patent law protects software from unauthorized copying, distribution, and sale. The law describing these copyrights and their limitations is included in Title 17 of the U. S. Code. Potential penalties for infringers are listed in both Title 17 and Title 18. The law also recognizes the Internet and prohibits users from uploading, downloading, or transmitting unauthorized copies of software online. An individual who breaks these laws, or a company that looks the other way when an employee does it, has civil and criminal liability. The consequences range from significant civil damages to criminal fines, and even the possibility of imprisonment.

Using illegal copies of software has other serious consequences. Software publishers offer their legitimate customers a wide array of services besides the program itself; these include support services, and upgrades. A legitimate copy or user account ensures that a purchaser is getting a quality product produced by the rightful owner.

An illegal copy or inappropriate account sharing provides none of these benefits. Further, it could contain malware that can damage or compromise data or a copy hiding a damaging virus capable of jeopardizing the security of an organization's computer network. Any one of these problems could quickly escalate into costly damages that become far more expensive than the money you "saved" by buying or downloading unauthorized software.

Management

How to Manage Software Properly

Unlicensed software and inappropriate account sharing cheat creators out of their reward for the innovation they have created; it also cheats a company out of the full value of the software. In addition, it can expose confidential data, create privacy concerns and subject the owner to criminal or civil penalties. In short, using pirated software is bad business for everyone.

Effective Management of Software is a Four-Step Process

Step One: Develop Policies and Procedures

Before anything else, a company culture of SAM must exist. In this culture, all employees must understand the value of software, learn the difference between authorized and unauthorized use, and commit to using licensed software. To do this, an organization must have a clear statement of policy. The statement should express the company's goals to manage software for maximum benefit, deal only in authorized software and spell out the procedure for acquiring authorized software. An effective software purchase procedure consists of the following elements:

- Centralize all software purchases, including services, through a purchasing department or other designated company authority.
- Require all software purchase requests, including services, be in writing and made available to the purchasing department or another agreed upon department.

It is important to educate employees on the role they play in protecting their company against security breaches. Senior management needs to play an active role in the information security programs of the organizations in order for them to succeed. The following security tips are important to keep in mind:

- Install Anti-Virus Software: Ensure that all computers have anti-virus software installed. Make sure the automatic update feature is activated.
- Be Cyber Secure: Report cyber-attacks to local law enforcement agencies and your IT provider.
- Install a Firewall: A firewall will protect devices from unauthorized access and use by hackers.
- Check for Security Updates: Security updates should be checked every 30 days for programs installed on computers and operating systems. Allow for automatic updating and/or subscribe to a notification service provided by the vendor.
- Computer Passwords: Change system passwords every 90 days and make sure they are strong passwords that contain both numbers and symbols.
- Employee Communication: Talk to employees about the importance of being cyber secure.

Manager approval;

- Ensure software being requested is on the company's list of supported software.
- Buy only from reputable, authorized sellers.
- Work only with reputable Application Service Providers (ASPs), and ensure all relevant licenses are maintained and documentation with that ASP.
- Get original user materials (e.g., manuals, registration cards, etc.), licenses, and receipts for each purchase.
- Do not permit employees to buy software directly or charge it to their expense accounts.

- Ensure that software cannot be downloaded from the Internet by employees without special approval.
- Do not permit employees to download peer-to-peer (P2P) client software that may be used for downloading content not authorized for installation on company resources.

There is a sample corporate policy statement at the back of this booklet for your company to consider adopting as its own. Whatever your policy, make sure it is included in the packet of information given to new employees, distributed to all current employees and posted on company websites. Every employee needs to acknowledge the statement of policy and the consequences of violating it. In turn, employers must take steps to educate employees on what constitutes illegal use of software.

In developing internal procedures for software asset management, every company should "what software do we need?" The answer will always be valuable in ensuring effective and efficient purchasing and use of software.

As a general principle, procedural analysis should answer the following questions:

- Is the right software in terms of efficiency and effectiveness being used?
- Is there other software programs or services that would enable staff to operate in a more effective and efficient manner?
- Is there software programs currently in possession but no longer needed?

Businesses procedures should identify the appropriate software profile for each computer by assessing if staff members need alternative or additional software applications. Software not being used should be identified to determine if that program should be maintained

Step Two: Audit Your Software

Once a policy and a set of procedures in place, the next step is to take inventory of all software assets. Only by knowing what programs are installed on all the devices in an organization including desktops, laptops, servers and any copies of programs from work installed by employees on their home computers, can a business determine how to proceed.

An accurate inventory can answer the following questions:

- Are we using the most recent or most suitable version of programs we need?
- Are we using outdated or unnecessary programs that can be deleted?
- Are there other programs or services we should obtain to become more productive or efficient?
- Does each employee have the correct set of available programs?
- Do we have illegal, unauthorized, or unlicensed programs or copies in our business?

There are many tools available to help complete the inventory or it can be done manually. BSA's website, www.bsa.org, provides third-party software audit tools free of charge to businesses. No matter what tools used, make sure to collect the following information for each copy of software installed on each computer or utilized via the Internet:

- Product Name

- Version Number
- Serial Number

Companies should also take an inventory of material related to software on computers including:

- CDs or other storage media used to install the programs.
- Account registrations for remotely accessed software.
- Original manuals and reference documentation.
- License documentation.
- Invoices, proofs of purchase and other documents proving the legitimacy of purchased software. This includes invoices for computer systems that were sold with software already installed.

Once the inventory is complete, you should carefully store the documentation, original copies of your software, and other material in a secure place. That way, you can take advantage of services, upgrade offers, and the like from publishers, and reinstall software or access accounts more easily.

Step Three: Determine What's Authorized or Unauthorized

With inventory in hand, compare the software installed on computers or utilized via SaaS to what's allowed under the terms of your licenses. Remember that some licenses allow for a certain number of copies of a program from a single source or allow a limited number of network users accessing the software or accounts simultaneously. The original license or service agreements will explain how many.

Once unauthorized software copies or improperly utilized account registrations have been identified, delete these or cease the account sharing. This is also an ideal time to remind employees about the company's software policy and the dangers associated with unlicensed software.

Now compare the legitimate copies of software and accounts with the corporate needs that identified when taking inventory. This allows for informed decisions about which software and accounts legally owned that should be kept, upgraded, or discarded. Programs can be moved —not copied — from computers where they are not needed to computers where they are. Programs can be upgraded, if necessary, so that everyone is using the version of the program that's most appropriate for your company. Now, only the new, legitimate software and accounts needed must be purchased.

Prevention

Preventing Software Piracy in the Workplace

Based on the inventory, upgrades, new purchases, and input from employees, create a formal list of the software and online services that your company will allow its employees to use. This should include program names, serial numbers, version numbers, number of copies or users permitted by the license, the computers on which the copies are installed, and plans to add, upgrade, or discard the software in the future.

Step Four: Establish a Routine Audit

Monitoring adherence, guarding against the introduction of unauthorized software and keeping a list of supported software and services up-to-date is a continual process. In many businesses, it makes sense to have someone, oftentimes called a SAM manager, responsible for the process in order to centralize the job.

Periodically, it's a good idea to perform spot checks on individual computers to ensure illegal software has not been inadvertently or deliberately installed. It also makes sense to conduct a software inventory at least every year, just as any organization would for other valuable assets. When employees leave the company, make sure the software they worked with remains within company and that the old employee does not take or keep copies.

Understanding License Compliance is Simply a Business "Best Practice"

After software assets are in good order, businesses still need to monitor their workplace for unauthorized software. There are four common types of software piracy, and understanding each will help avoid the problems of illegal software.

End-User Piracy

End-user piracy occurs when an employee reproduces copies of software without authorization. End-user piracy can take the following forms:

- Using one licensed copy to install a program on multiple computers.
- Copying disks for installation and distribution.
- Taking advantage of upgrade offers without having a legal copy of the version to be upgraded.
- Acquiring academic or other restricted or non-retail software without a license for commercial use.
- Sharing account or service access information.

The lion's share of the losses due to software piracy comes from the relatively pedestrian problem of over-installation—that is, loading program on to more computers than is authorized by the license agreement. Piracy not only deprives software creators of a return on their investment, it costs jobs in related businesses, hurts the economy, and deprives the consumer of new products.

Technological measures to stem the growth of piracy are rapidly becoming a mainstream option from many software companies. Technologies such as product activation help ensure compliance with end-user license agreements, while minimizing the impact on legitimate users. One simple step in the installation process is often all it takes to enable full use of a software program and to prevent its unauthorized installation. Product activation technologies that are fast, nonintrusive, anonymous and flexible help combat piracy without unduly burdening users.

Certified Professionals

SAM Advantage (samadvantage.bsa.org) is the industry's first ISO standards-based SAM training course. Targeted at the IT manager / SAM professional, the course provides complete guidance and best practices used to develop and institute ISO-aligned SAM processes within an organization. Additional information is available at samadvantage.bsa.org.

Cloud Piracy

While the impact from piracy is reduced for purely cloud-based software companies, such theft will take unique forms and remain persistent for companies that take a "hybrid" approach (i.e. using cloud and traditional delivery models). BSA expects software theft in the cloud to take several forms. Some of these forms are entirely new; others are simply updated variations of existing problems. They include: web-based distribution of pirated software piracy and under-licensing in a private cloud model; public cloud distribution of software without a license to redistribute; and, SAAS subscription abuse.

Internet Piracy

Software publishers have contributed in countless ways to the Internet's success, providing the means by which content can be created, displayed and exchanged, and providing some of the most desired content itself. However, IP theft on the Internet constrains the software industry and significantly reduces its positive impact on the world economy. There are thousands of pirate websites on the Internet, and virtually every commercial software product now available on the market can be located on one of these sites.

More on Internet Piracy

BSA's global Internet page, internet.bsa.org, provides up-to-date information about the threats associated with internet piracy. The site has an extensive news section to learn about the most recent threats that software users need to know.

The same laws and license agreements that apply to software in physical distribution channels also apply to cyberspace and Internet transactions. The U. S. Copyright Act does not differentiate between offline and online infringement. Both are prohibited and subject to criminal prosecution and civil penalties, including statutory damage awards of up to $150,000 per copyrighted work.

While there are many publishers who offer authorized versions of their software for sale online, there are also numerous pirate operations on the Internet as well. These include:

- Pirate websites that make software available for free download or in exchange for uploaded programs.
- Internet auction sites that offer counterfeit, out-of-channel, or infringing copyright software.
- Peer-to-Peer networks that enable unauthorized transfer of copyrighted programs.

The purchasing rules that apply to software purchased through traditional means should also apply to online software purchases. Organizations should have a clear policy as to when, if, or with whose authorization employees may download or acquire software from Internet sites.

Below are tips to help the businesses and the public when purchasing software online from auction sites, discount retailers, or in response to email solicitations:

- If a price for a software product seems "too good to be true," it probably is.
- Be wary of software products that come without any documentation or manuals.
- Beware of products that do not look genuine, such as those with handwritten labels.
- Beware of sellers offering to make "backup" copies.
- Watch out for products labeled as academic, OEM, NFR, or CD-R.
- Be wary of compilations of software titles from different publishers on a single disk.

- Do not give out your credit card details unless you know it's a secure transaction.
- Check with organizations such as BSA should you become a victim of software fraud.

Software Counterfeiting

Software counterfeiting is the illegal duplication and sale of copyrighted material with the intent of directly imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the CDs incorporating the software program, as well as related packaging, manuals, license agreements, labels, registration cards, and security features. Sometimes it is clear the product is not legitimate, but often it is not. Look for the following warning signs:

- You're offered software at a price that appears "too good to be true.
- The software comes in a CD jewel case without the packaging and materials that typically accompany a legitimate product.
- The software lacks the manufacturer's standard security features.
- The software lacks an original license or other materials that typically accompany legitimate products, for example the original registration card or manual.
- The packaging or materials that accompany the software have been copied or are of inferior print quality.
- The software is offered on an auction site.
- The CD has a gold appearance, rather than the silver, blue, or green appearance that characterizes a legitimate product.
- The CD contains software from more than one manufacturer or programs that are not typically sold as a suite.
- The software is distributed via mail order or online by sellers who fail to provide appropriate guarantees of a legitimate product.

CONCLUSION

Proper software asset management takes time and effort, but the payback is well worth it. If you have followed the process outlined in this guide, you have taken the steps necessary to get the full benefit from purchased software and eliminate your company's exposure to penalties for illegal software usage.

About BSA | The Software Alliance

The BSA | The Software Alliance (www.bsa.org) is the leading global advocate for the software industry. It is an association of nearly 100 world-class companies that invest billions of dollars annually to create software solutions that spark the economy and improve modern life. Through international government relations, intellectual property enforcement and educational activities, BSA expands the horizons of the digital world and builds trust and confidence in the new technologies driving it forward.

BSA's website offers a variety of information on software management, security, policy initiatives, and copyright issues around the globe. BSA also operates 65 anti-piracy hotlines around the world for those reporting suspected software thefts.

BSA | The Software Alliance
20 F Street, NW, Suite 800
Washington, DC 20001
Tel: 202. 872. 5500
Fax: 202. 872. 5501
Hotline 1. 888. NO. PIRACY

BSA Europe/Middle East/Africa
2 Queen Annes Gate Bldgs.
Dartmouth Street
London SW1H 9BP
United Kingdom
Tel: +44 (0) 20. 7245. 030
Fax: +44 (0) 20. 7245. 0310

BSA Asia
300 Beach Road
#32-07 The Concourse
Singapore 199555
Tel: + 65. 6. 292. 2072
Fax: + 65. 6. 292. 6369

SAMPLE A

(Note: This document is intended to be used and customized to your needs.)

Corporate Software Policy

Corporate policy regarding the use of personal computer software.

1. (Organization) licenses the use of computer software from a variety of outside companies. (Organization) does not own this software or its related documentation, and unless authorized by the software developer, does not have the right to reproduce it except for back-up purposes.
2. (Organization) employees shall use the software only in accordance with the license agreements and will not install unauthorized copies of commercial software.
3. (Organization) employees shall not download or upload unauthorized software over the Internet.
4. (Organization) employees learning of any misuse of software or related documentation within the company shall notify the department manager or (Organization)'s legal counsel.
5. According to applicable copyright law, persons involved in the illegal reproduction of software can be subject to civil damages and criminal penalties including fines and imprisonment. (Organization) does not condone the illegal duplication of software. (Organization) employees who make, acquire, or use unauthorized copies of computer software shall be disciplined as appropriate under the circumstances. Such discipline may include termination.
6. Any doubts concerning whether any employee may copy or use a given software program should be raised with a responsible manager.

I am fully aware of the software use policies of (Organization) and agree to uphold these policies.

_____ _____

Employees Signature Date

SAMPLE B

Memorandum to Employees

To: (specify distribution)

From: (CEO or Senior Management Official)

Subject: Computer Software and U. S. Copyright Law

Date: (insert)

The purpose of this memorandum is to remind you of (Organization)'s policy concerning the illegal copying and use of commercial software. Unlicensed duplication or unauthorized use of any software program is illegal and can expose you and the company to civil and criminal liability under the copyright law.

To ensure that you do not violate the software publisher's copyright, do not copy any program installed on your computer for any purpose without permission from (insert name of responsible manager or department). Do not install any program on to your computer without such permission or clear verification that the company owns a license to cover that installation. Finally, do not download unauthorized software from the Internet.

- (Organization) will not tolerate any employee making unauthorized copies of software.
- (Organization) will not tolerate any employee downloading or uploading unauthorized software from the Internet including, but not limited to, downloading peer-to-peer (P2P) client software that may be used for trading copyrighted works.

Any employee found copying software illegally is subject to termination from (Organization).

- Any employee illegally copying software to give to any third party, including clients and customers, is also subject to termination.
- If you want to use software licensed by (Organization) at home, you must consult with (insert name of manager) in order to make sure such use is permitted by the publisher's license.

This policy will be strictly enforced to make ensure all employees and (Organization) are not exposed to serious legal consequences.

(Organization) will periodically inventory software on all company owned devices to ascertain that (Organization) owns licenses for each copy of a software product. If unlicensed copies are found, they will be deleted, and if necessary, replaced with licensed copies.

Please do not hesitate to contact me if you have any questions.

SAMPLE C

Software Needs Analysis Form

Employee Information:

Name: Department: Authorization: Date:

Computer serial number and location:

Current Software:

Software Program	Publisher	Version	Usage (Daily, Weekly, Monthly, or Never)

Is there software that you feel you need but don't have, which will assist you in your job? Please list below.

1:

2:

3:

www.bsa.org