

Never Fear Another Software Audit

Three pillars of effective asset management

Never Fear Another Software Audit

Three pillars of effective asset management

Contents

Executive Summary	1
Introduction	1
Complexity	1
Virtualization	1
Fragmentation of responsibility	2
Inadequate management	2
Alternative approaches	2
Do-it-yourself methods	2
Point solutions	3
Enterprise Resource Planning solutions	3
Software provider solutions	3
Three pillars of effective asset management	3
1. Efficiency	3
2. Effectiveness	4
3. Control	5
A proven audit support solution	5
Efficiency—ITIL compliant CMDB	5
Effectiveness—Simplified license management	6
Control—Built-in process automation	6
Conclusions	6

Executive Summary

Software audits are disruptive, risky—and unless you're prepared, the vendors have all the leverage. Software inventory and management tools can help you keep track of licenses and avoid audits, but beware of the shortfalls of do-it-yourself, narrow, accounting-focused, or vendor-supplied solutions. An effective asset management solution is efficient, effective, and keeps you in control. Look for an Information Technology Infrastructure Library (ITIL) compliant Configuration Management Database (CMDB), simplified license management, and built-in process automation when selecting your solution.

Introduction

Software vendors use license audits to make sure customers stay in compliance with contracts they signed. For suppliers, they are a legitimate way to protect software products that are both valuable and vulnerable to instant, limitless copying. But for customers, license audits are intrusions that pull resources from important projects and add no business value of their own. They trigger the worst kind of IT fire drill, require participation from multiple departments, draw lots of executive attention, and launch endless meetings.

Software license audits are on the rise¹—and so are disputes and noncompliance claims. Some analysts suspect vendors used audits to meet revenue targets during the economic slowdown.² But even in good times, threats of audit exposure are sometimes used as tactics in pricing and support negotiations, for example when vendor sales teams pressure customers to agree to “informal” audits³ to break loose purchases of extra licenses, larger bundles, or extended support.

There's plenty of compliance risk to go around, even without invoking vendor misconduct. Four main contributors are:

Complexity

- Companies spend 20 percent or more of their IT budgets on software licenses⁴, much of it on operating systems (OS), virtualization platforms, and office productivity applications encompassing hundreds or thousands of instances.
- Even a single software title may be deployed in multiple versions, each carrying its own license terms and conditions.

Virtualization

- With no industry-standard way to apply these metrics to virtual domains, organizations can inadvertently put themselves out of compliance through well-intentioned efforts to improve efficiency and utilization.
- Virtual servers and streamed applications add another layer of complexity.
- Software licenses were developed using hardware “per-processor” and other metrics.

1-Thomas Wailgum. “Software Audits on the Rise: Survival Tips”, CIO Magazine. (Framingham, MA: CXO Media Inc., January 6, 2010). <http://www.cio.com/article/print/512818>

2-Wailgum, Software Audits.

3-Chris Kanaracus. “Software License Audits Come in Multiple Flavors” CIO Magazine. (Framingham, MA: CXO Media Inc., September 18, 2009). <http://www.cio.com/article/print/502566>

4-Bona and Disbrow, License Audits.

Never Fear Another Software Audit

Three pillars of effective asset management

Fragmentation of responsibility

- Responsibility for software license management spans an organization's IT staff, Legal, Purchasing, and Financial departments, as well as end users.
- Physical documentation of purchases and entitlements may be distributed in offices around the world, and undocumented user downloads compound the risk.
- One-at-a-time management of procurement requests creates bottlenecks for any large IT organization, and encourages noncompliant downloads and untracked personal or "maverick" purchases.

Inadequate management

- Rushing to get new users and applications in production, organizations may neglect installation monitoring and license tracking, raising audit risks.
- Failure to monitor application usage adds cost and risk from software instances that create no business value.
- Poor end-of-life management often leaves organizations paying fees for software long after it has been replaced and removed.

Almost every IT trend—faster networks, greater storage volume, virtualization, cloud computing—makes software asset management more difficult, and audits more frequent and painful. New initiatives such as cash rewards for turning in noncompliant companies⁵ demonstrate vendors' determination to hold their ground.

Audits sustain an unbalanced, adversarial relationship in which vendors not only set the pricing and penalties, but control how licenses are counted, and even control the discovery tools that do the counting. Audit-driven compliance processes inevitably compromise the free exchange of information with vendors, so organizations not only pay more for software, but get poorer communications, service, and support.

To restore their balance of power with software vendors, customers need to take charge of their software assets, starting with discovery and inventory and extending through full lifecycle management. Unfortunately, many of the approaches they take are little more than half measures that do little to reduce the workloads associated with software license audits, and the associated risks.

Alternative approaches

Most IT organizations already have some capability to manage their most important IT assets—to complete financial reports, for example, or keep track of upgrade and refresh cycles. But the solutions they use often rely on time-consuming manual processes, or are poorly adapted to managing non-physical assets like software. These are the most common approaches:

Do-it-yourself methods

Scripts and spreadsheets were the norm for asset management a decade ago, and some of them survive. But most IT organizations now recognize that the time and effort spent on input and maintenance of these one-off solutions would be better applied to customizing a full-featured, integrated management suite to their individual requirements.

5-Business Software Alliance. Report Piracy Now! (Web page). (Washington, DC. 2010). <https://reporting.bsa.org>

Never Fear Another Software Audit

Three pillars of effective asset management

Point solutions

There is no shortage of narrow-focus management solutions, and some of them are free. These are essentially do-it-yourself methods that were developed by someone outside your organization. As a result, they suffer from the same data entry and maintenance issues, and often lack customization capabilities.

Enterprise Resource Planning solutions

Enterprise Resource Planning (ERP) solutions track assets for financial accounting and tax purposes, and some providers have added extensions that help manage IT assets. However, the asset discovery and workflow capabilities of these packages are rudimentary, and they weren't designed to support advanced IT management functions like configuration management. From an IT perspective, ERP should be a client of the asset management solution—not the host.

Software provider solutions

Providers of major operating systems, databases, and productivity solutions often offer discovery and inventory tools to help their customers manage licenses. But these solutions are seldom compatible with other providers' software, leaving IT to struggle with different user interfaces, data definitions, workflows, and more. And using a providers' own tools to collect information that will be used in a tough audit or sales negotiation is a risky business practice.

Integrating all of these individual tools is a significant problem. Answering even a simple business question typically means patching together data from multiple solutions, wasting time and risking errors. Worse, these solutions miss a significant opportunity for sustained improvement in IT operations. Asset discovery and inventory can be the first step toward comprehensive management of software and hardware assets across providers, locations, and asset lifecycles. A fragmented approach using multiple tools—even when it gets IT through a license audit—returns them to the starting point for the next iteration.

Three pillars of effective asset management

Disciplined asset management often starts with efforts to cut the time, effort, and risk of software licensing or financial compliance. This approach is almost immediately effective, but it is only the start of what asset management can do. In a companion paper, we discuss the strategic and financial benefits of asset management (please see the sidebar for details). Our purpose here is to show how a mature, automated asset management solution helps IT departments get and stay ahead of license audits, makes their staff more efficient and effective, and keeps them in control of expensive software assets.

1. Efficiency

Asset management processes discover, inventory, and track the elements that make up IT infrastructure—hardware as well as software.

- Creating a map of the IT universe is the key to software license compliance.
- Armed with advance knowledge and credible documentation of the location and license status of every important OS, virtualization platform, or application instance, specialists can quickly identify problems, apply solutions, and move on.

Never Fear Another Software Audit

Three pillars of effective asset management

Discovery and tracking—Automated solutions accelerate or eliminate many of the time-consuming, mundane, or simply impossible tasks involved in discovering the presence, location, context, and status of software assets. Integrating electronically discovered information with data imported from other systems, spreadsheets, databases, and barcodes from product packages and hardware asset tags helps organizations build a CMDB for accurate, up-to-date inventory of hardware and software assets, with their relationships to one another.

Inventories—The CMDB contains detailed, up-to-date information about the applications installed across multiple networks, and the licenses are associated with them, for comparison with data from license agreements, financial records, and vendor sales records. Automated reports organize compliance information quickly to meet enforcement agency requirements—so you can get back to productive work.

2. Effectiveness

Discovery and reporting tools help organizations complete audit preparation tasks quickly and well under pressure.

- Process automation workflow templates helps organize tasks into effective processes, orchestrating interactions among individuals, systems, and groups, reducing administrative burdens on IT staff.
- Workflow templates are particularly useful for license compliance processes that cross organizational boundaries.
- Track usage at the product level to facilitate license harvesting for underutilized software.

Audits aren't the only impact of software licensing on your IT operations. Direct costs, loss of negotiating leverage, and exposure to compliance risks from virtualization and data center growth can all result from poorly-managed software assets. Ask your Symantec representative for a copy of our companion paper, *Stop Sacrificing Your IT Budget on Software*, and learn the ten steps you can take now to free your budget of software costs that aren't contributing their fair share of business value.

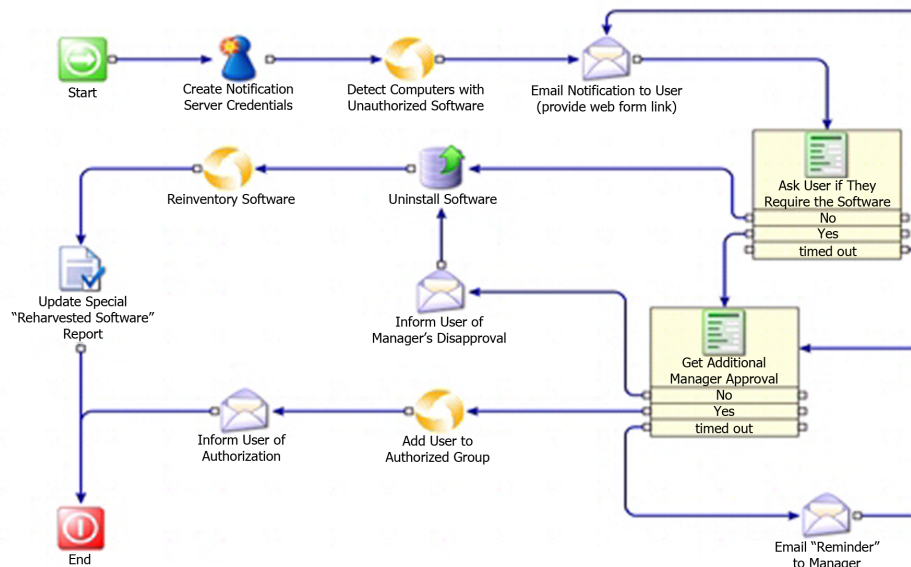


Figure 1: Sample automated workflow: software license harvesting.

Never Fear Another Software Audit

Three pillars of effective asset management

Hardware and software requests—Asset management workflow templates automate and track procurement approvals across departmental lines, with links to financial and inventory systems. It batches approvals and automates notifications, for big increases in throughput and user satisfaction, and maintains links between software instances, purchase records, license terms, and entitlement documentation throughout the software's useful life.

Lease termination—Defined process automation workflows assure that end-of-life assets are properly retired, including the often-neglected steps of lease termination for software, and secure disposal of hardware.

3. Control

A CMDB provides an accurate, up-to-date picture of assets under management, augmented by effective automated processes that unlock the business value of IT, particularly during periods of rapid growth or change. Software vendors are aware that reorganizations involve significant reassignment of software and other assets, and may be more likely to schedule audits after such events. Rapid growth, from a merger or acquisition, can be almost as disruptive as downsizing.

Growth and change— Asset management solutions help streamline employee on-boarding in times of growth, speed asset reallocation in times of contraction, and automate record-keeping to document compliance through both. And predefined workflows accelerate the time-to-value of new or reassigned IT staff.

Documented compliance—A full, standards-based asset management solution integrates all information pertinent to software license compliance into the CMDB, and keeps the information accessible through predefined reports, with drill-down detail to document software instances, versions, serial numbers, associated systems and users, licenses, entitlement documentation and much more. It balances the information and power relationships across the table during a software audit, minimizes the disruption they cause, and may help organizations avoid them altogether.

A proven audit support solution

Altiris™ Asset Management Suite from Symantec is the asset management component of Symantec's comprehensive, modular IT Management platform. Built around a CMDB in conformance with the Information Technology Infrastructure Library (ITIL), the solution offers:

- Vendor-neutral, independent tools for discovery, inventory, and tracking of software and hardware assets.
- Comprehensive reports to meet the most demanding requirements of vendor software license audits.
- Pre-built, customizable workflow templates optimize and automate time-consuming IT administrative tasks.

Already a proven IT management solution, Altiris™ Asset Management Suite adds a new user interface and software catalog, including these features to simplify and accelerate license compliance:

Efficiency—ITIL compliant CMDB

- Gain visibility into real-time asset information from a single source.
- This single source, the CMDB manages hierarchical relationships of assets, including assets to other configuration items, users, locations, departments, cost centers, and associated contracts.

Never Fear Another Software Audit

Three pillars of effective asset management

Effectiveness—Simplified license management

- Graphic display of software immediately shows over- or under-deployment and compliance.
- Easy integration of deployment and usage information with purchasing records, financial data, and entitlement documentation.

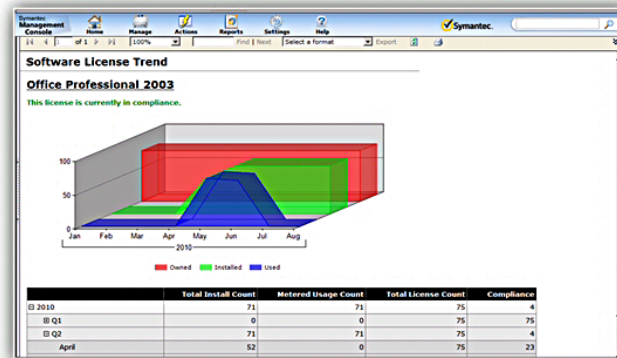


Figure 2: Simplify license management: visually track licenses owned, versus installed, versus used

Control—Built-in process automation

- Incorporate non-Symantec technologies such as HR and finance systems, for process automation across departments and systems.
- Custom process orchestration that one customer used to save \$2M in license fees and 18 months of project time using just one automated process.

Conclusions

Many organizations get serious about asset management in response to an expensive audit. Asset management is one of the fastest ways for IT to protect against compliance risks and save the organization a lot of money, but it's only a start. Asset management is the starting point for disciplined, standards-based management that elevates IT's efficiency, effectiveness, and control—and ultimately, the business value and career satisfaction of IT professionals.

About Symantec

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

For specific country offices and contact numbers, please visit our website.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.
3/2011