

## Making PC Lifecycle Management Work for You

### A Four-Phase Approach

---

#### CONTENTS

Evolution of Desktop Management .....	1
Why Traditional Desktop Management Doesn't Work .....	2
How to Approach Each Phase of the PC Lifecycle .....	3
Phase 1: Readiness .....	3
Phase 2: Deployment .....	4
Phase 3: Management .....	5
Phase 4: Retirement .....	6
The Path to Effective PCLM .....	7

---

# Making PC Lifecycle Management Work for You

## A Four-Phase Approach

Industry analyst Gartner estimates that 80 percent of the total cost of PC ownership is incurred after purchase, falling somewhere between \$7,000 and \$13,000 per PC per year. For many IT organizations, there is no higher priority than gaining control of this astronomical cost.

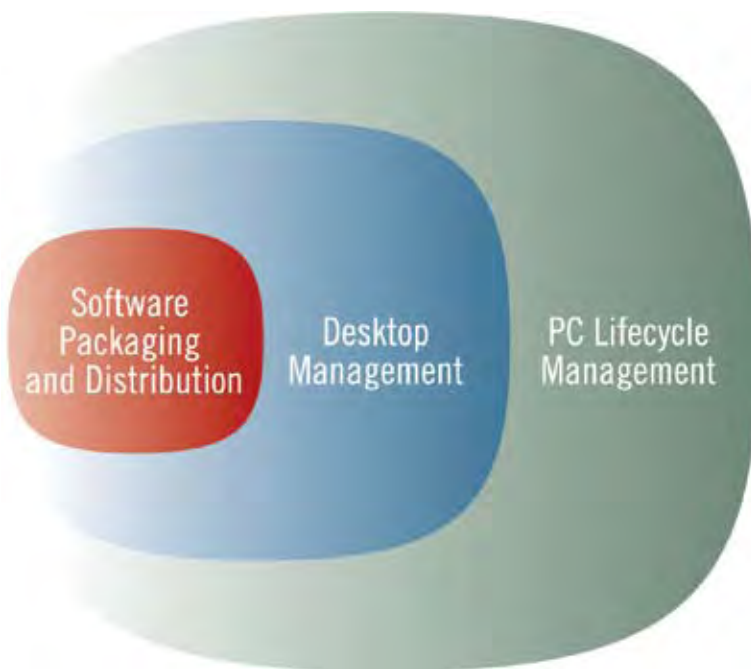
But that's easier said than done. Here's why: The needs of IT—for control, standardization, and analysis—often conflict with the needs of users—for flexible solutions, availability, and responsiveness. Over the years IT groups have used various desktop management solutions to tackle the problem, with limited success.

Today, PC lifecycle management (PCLM) provides a cohesive and effective solution. PCLM is the practice of managing end-user systems from purchase to retirement. It covers everything from initial deployment to upgrading, patching, and decommissioning your systems. Though it sounds like traditional desktop management, PCLM is different in one key way: It requires that you integrate your management process with your management product. Without this integration, PCLM will not work.

This white paper summarizes the evolution of desktop management, describes the problems associated with traditional desktop management approaches, and offers guidelines for approaching each stage of the PC lifecycle. As a result, you'll be able to more effectively preserve your PCLM investment and decrease your long-term PC ownership costs.

### Evolution of Desktop Management

The management of desktop and notebook computers has evolved from isolated, task-oriented solutions to an integrated set of automated management processes. Once centered around basic application packaging and deployment, desktop management now covers inventory and asset management along with all facets of the PC lifecycle: vulnerability and patch management, OS migration and deployment, hardware refresh, change management, system repair and recovery, and PC decommissioning.



## Why Traditional Desktop Management Doesn't Work

A natural conflict has always existed between the needs of IT and the needs of end users. This conflict surfaces, for example, when an organization needs a new application to support new products or services.

IT wants to control the new application environment by ensuring that it is standardized, thoroughly tested, and gradually deployed. In this way, they can avoid support headaches related to training, high error rates, and compatibility as well as security risks and license-compliance violations.

Most end users, on the other hand, are not interested in standardization. They prefer flexible solutions that will meet their diverse needs—based, for example, on departmental, operating system, or configuration requirements. Furthermore, users expect a quick turnaround time. Their schedules, correspondence, contact lists, presentations, and work in progress all reside on the PC. The faster they're up and running, the better.

For years, IT administrators have tried, without success, to strike a balance between complete lockdown and configuration anarchy. The approaches they've tried and their corresponding problems are described below.

### Manual processes

Manual processes, such as those based on scripts, have the following problems:

- Scripting is time consuming, provides little to no reporting, and is usually executed only upon user login. It may also require end-user interaction.
- Scripting does not usually accommodate event capture, validation, and rollback. As a result, it's difficult to confirm whether a process was successful before returning to a desired state.
- Scripting requires more IT resources, and thereby costs more, than automated processes.
- Scripting results in lost opportunity costs when IT spends time dealing with repetitive issues rather than proactively solving strategic problems.

### Nonintegrated point solutions

Using a different, nonintegrated tool for each management task (patch management, software distribution, hardware or software inventory, and OS installation) is problematic for these reasons:

- Multiple, directly related PCLM tasks cannot be linked together into common workflows. For example, inventory, patch management, software packaging, and distribution are co-dependent tasks and should be leveraged within the same management infrastructure.
- The combined license cost per tool (i.e., patch, inventory, and asset management solutions as well as the necessary hardware) can far exceed that of an integrated offering.
- Nonintegrated tools do not lend themselves to a repeatable process and nearly always require multiple visits to the PC.
- The use of stand-alone tools does not provide a consolidated repository and view of your hardware and software assets or the resulting management activities. Providing comprehensive reports or analysis cannot be accomplished since information about different tasks—such as patches deployed, applications deployed, and hardware configurations—are scattered across different databases.

### Misuse of imaging

Disk imaging software, one of the most popular and powerful PC utilities available, is frequently misused for software distribution, data backup, and patch management—tasks that it was not designed to perform.

Many IT organizations have discovered that their use of imaging as a primary method for application and operating system deployment has created a large and unmanageable library of images requiring continuous updating and maintenance.

In fact, Gartner has found that an organization with 2,500 PCs creates an average of 20 new images each year. With PCs being changed every four years and notebooks being changed every three years, the result is a total of 70 images needing yearly maintenance. The annual fixed cost to create and maintain these 70 images is approximately US\$ 380,000 (Gartner Research, *Saving Money on PC Deployment*, Michael A. Silver, 8 December 2005).

That's not to say that imaging does not play a useful role. It does, but only when it is used to generate "thin images" or "standard operating environment images." If you are using a disk imaging solution (such as Norton Ghost™) to manage anything other than operating system distribution, you probably won't realize true automated software distribution, patch management, or PC disaster recovery. In fact, you may end up managing images instead of PCs.

Given the number of PC hardware configurations, operating systems, and applications in most organizations—along with the weekly stream of Microsoft patch updates, anti-virus updates, OS upgrades, user-based software installations, and configuration changes—it’s clear that the task of managing PCs has become too complex and too important to be handled on an ad-hoc basis.

## How to Approach Each Phase of the PC Lifecycle

PCLM cannot be purchased; it must be practiced at each phase of the product lifecycle. Like all other assets, PCs are acquired and then eventually retired. Most of the total cost of ownership is absorbed by the activities that occur after procurement.

These activities can be broken down into four phases: Readiness, Deployment, Management, and Retirement. You can effectively approach each phase by following these guidelines:

### Phase 1: Readiness

You can begin the Readiness phase by conducting a thorough inventory and analysis of your current PC hardware and software assets. Make sure to use an inventory tool that provides reliable data, powerful

reporting, and integration with other PC management tasks. The ability to automatically discover machines through an existing Active Directory or non-Active Directory network is particularly important.

Once you have a clear view of your hardware and software assets, you can develop plans and policies for managing those assets going forward. You’ll want to address these critical areas:

- **License compliance and usage**

When you know which applications are being used and how often, you can determine whether unused licenses should be reallocated or additional licenses need to be provisioned. In the process, you can also rectify potential license compliance issues. (For more about license compliance, see *Phase 3: Management* in this paper.)

- **Hardware configuration**

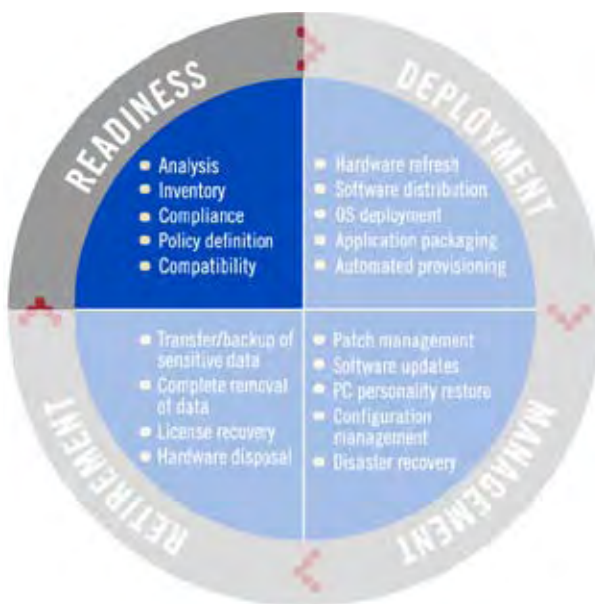
Inventory reports provide detail on existing PC hardware configurations (video hardware, memory, CPU, hard disk space, etc.) and help you determine whether your hardware can support the operating system and applications to be deployed. With this information, you can also establish PC acquisition policies and cost forecasting to help avoid reactive and sporadic PC purchases.

- **Policy definition**

Using the information gained from your environmental analysis, you can begin to define policies around network and application access. You can also plan for the implementation of managed policy configurations, addressing items like PC power management, control panel applet access, and security risks (for example, increasing security by locking down removable storage devices).

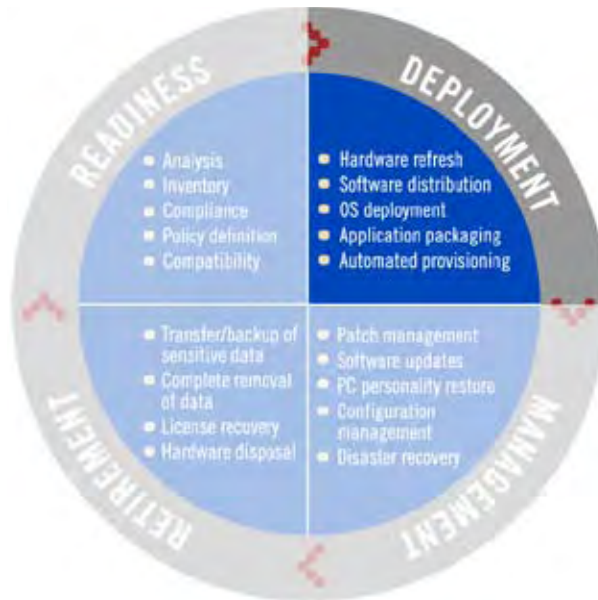
- **Compatibility**

By configuring test environments and IT labs to match user work spaces, you can thoroughly test new applications, patches, and updates before deployment.



## Phase 2: Deployment

After you have initiated policies and procedures based on asset analysis, you can begin to develop strategies around PC deployment, including operating system deployment, application packaging, software distribution, patch management, data backup and restore, and corporate network configuration.



These naturally interdependent tasks are often performed in isolation using manual-build processes or disjointed tools and utilities. With the support of a well-integrated PCLM solution, you should be able to implement an automated PC deployment process that minimizes or even eliminates any hands-on interaction from IT staff.

Three primary scenarios drive the need for automated or zero-touch PC deployment:

- **PC migration:** An existing PC is migrated to a new operating system.
- **PC refresh:** A new\* PC replaces an old PC.
- **New user:** A new\* PC is deployed to a new employee.

\* The term "new PC" does not always refer to a brand new PC fresh from the manufacturer. It could refer to a previously used PC that was returned to inventory and then redistributed to an existing or new employee.

The list below outlines the processes that need to be integrated for automated deployment to be effective:

- **Application packaging**  
Unfortunately, many organizations overlook this important task only to discover that an improperly packaged application is highly problematic. In addition to causing potential system conflicts, it limits your ability to provide automatic distribution, cannot easily be integrated with a patching process, and creates challenges with automated uninstall.
- **OS deployment and software distribution**  
You can eliminate errors that typically occur with imaging or OS upgrades by implementing zero-touch, automated bare-metal provisioning of operating systems to new PCs or during OS migrations. Furthermore, a properly packaged application provides flexible deployment options, such as scheduled, inventory-based, interactive, automatic, and Internet installer. Be sure to keep distribution methods consistent across the organization to avoid over-deployment of licenses.
- **Remote PCs and unreliable networks**  
To ensure reliable delivery of application packages to managed PCs, especially over slow, unreliable networks, and to mobile or remote users over VPNs, you need the following options: two-phase installation, check-point restart, multi-cast/unicast options, and bandwidth throttling.
- **Joining the network**  
Once operating systems and patches have been deployed to PCs, you should have the capability to automatically configure network and domain properties.
- **PC personality backup and restore**  
You need to be able to capture the PC personality (bookmarks, shortcuts, documents, customized dictionaries, e-mail settings, printer settings, and drive mappings) so that it can be automatically migrated to the new PC. Without this step, IT staff and users may spend hours trying to reconfigure these settings for the new and possibly unfamiliar operating system.
- **PC lockdown**  
Every time an employee uses a removable storage device such as a USB flash drive, external hard drive, or even an iPod, or loads software with unknown security properties, there's risk involved.

But locking down the PC is tricky. Although Windows® 2000 and XP Professional are built to enable lockdown, they have also been inhibitors because many applications require administrator access in order to execute properly on these operating systems.

Windows Vista™ will attempt to address this problem through User Account Control (UAC), but it will be years before we see a widespread adoption of Vista and just as long before software applications are updated to leverage UAC. In the meantime, Group Policy Objects (GPO) and third-party extensions are another way to enforce lockdown by selectively restricting activities for users, regardless of their privilege level.

**Phase 3: Management**

Downtime costs organizations billions of dollars annually. Virtually every employee relies on a core set of applications to perform his or her duties. Having those applications crash, even if only for a few hours, can cost a company hundreds of thousands of dollars in lost productivity and help desk costs.



Proper maintenance of the PC environment ensures that PCs have the most current operating system patches and updates, including security updates, and reduces the likelihood of crashes. In addition to supporting end users and managing both scheduled and unscheduled downtimes, the following tasks and issues must be addressed on an ongoing basis:

- OS updates**  
 Delivering new service packs, handling OS migrations, or restoring the OS on a failed PC helps to prevent lost productivity for the end user. Similarly, seamless delivery of a complete OS or OS updates helps to ensure that applications are not adversely affected and that user state and PC personality are seamlessly restored.
- Application updates**  
 The deployment of updated applications is best executed with a single integrated process. To ensure the best possible application uptime, uninterrupted user productivity, and reduced help desk calls, your software installation processes should also ensure automatic self-healing if an installation is corrupted for any reason.

- Vulnerability and patch management**  
 Organizations can no longer afford to rely on time-consuming and outdated manual security processes. Security experts estimate that over 90 percent of all viruses target known operating system and application vulnerabilities. For that reason, be sure to build your security reviews and patches into your overall application packaging and distribution process.

The benefit of a comprehensive PC lifecycle management solution is that it will use the same directory services, logging facilities, and reporting facilities to assess security vulnerabilities and accurately report security compliance.

- PC restoration**  
 A repeatable PC restoration process enables help desk personnel to quickly resolve problems by rebuilding PCs on-the-fly, from a central location, in order to decrease call resolution time or reduce the need to dispatch a technician to a PC.

When a user’s PC gets corrupted, a bold but effective policy is for the IT department to set a time limit (e.g. 30 minutes) that IT staff will work on the PC before the machine is restored to a known state. This practice is often faster than isolating and diagnosing the problem. It also sends an important message to users: If you’ve added applications or hardware devices that have corrupted the machine, IT will spend only a limited amount of time fixing the problem—and you will be responsible for reinstalling unsupported applications or components.

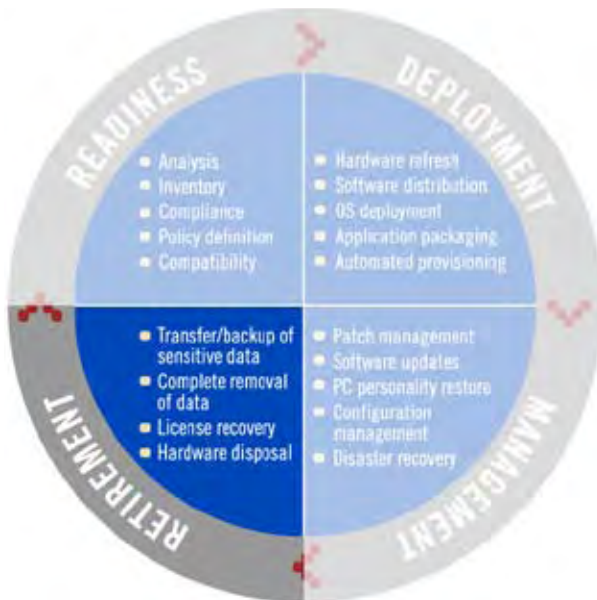
- **License compliance**

As organizations grow organically or through mergers and acquisition, tracking the deployment and use of software licenses becomes significantly more challenging. Because software can be deployed in so many different ways, over-deployment or over-purchasing can quickly get out of hand. Over-deployment, in particular, can jeopardize an organization's privacy, profits, and reputation.

You can avoid the risks of noncompliance with a solution that provides real-time trend analysis, cost analysis, detailed software usage analysis, graphical reporting, intelligent license utilization forecasts, and proactive compliance alerting. What's more, by conducting initial license auditing you can ensure accurate forecasting and lay the foundation for meaningful contract negotiations.

**Phase 4: Retirement**

PCs are removed from service at various times and for various reasons: physical failure, inability to run new applications or operating systems, lease expiration, planned obsolescence, or downsizing. Each of these reasons dictates a different process for retirement or disposal, depending on whether the asset is taken out of service and replaced with newer technology, returned to inventory, returned to the manufacturer or leasing organization, or recycled.



**The Scalable WinINSTALL Desktop Availability Suite**

WinINSTALL® Desktop Availability Suite is a comprehensive, tightly integrated management tool for automatically deploying, updating, tracking, and supporting PC hardware and software assets. Flexible by design, WinINSTALL is redefining desktop management by:

- Handling all the essential desktop management functions, from software distribution to patch and asset management.
- Providing high desktop availability and ensuring compliance with internal and external policies.
- Automating most labor-intensive desktop management tasks, including PC hardware deployment, OS migration, and PC recovery.

With these capabilities, you can effectively manage the PC lifecycle—from purchase to retirement.

The retirement process should involve participation from the end user, the IT organization, asset management group, facilities, finance, and one or more suppliers to handle the retired PC. Although the processes used may vary by company, certain critical tasks need to be addressed in the disposal process. The list below outlines key elements of a retirement or disposal process:

- **Inventory**

The first step of the retirement process is to scan the machine for license data that can be automatically captured and used to update asset management and compliance records. Many companies are immediately at risk because they fail to take this step. Once the PC is removed from the network, it is unavailable for automated inventory or scanning unless it is reattached to the network.

- **Data capture and storage**

By capturing intellectual property and business-critical data for future reference or reuse, you can prevent critical information from becoming lost or trapped in a PC entering the disposal process.

- **User state or PC personality**

Capturing user-defined PC settings and documents is especially crucial when replacing a user's PC with a new system. Automating the capture of PC personality and restoring it to the

new PC will save the end user and IT hours of time spent reconfiguring bookmarks, shortcuts, custom dictionaries, desktop settings, documents, and address books.

- **Sanitizing hard drives**

Unlike data capture and storage, the sanitizing process completely and irrevocably eliminates data from a hard drive. This is an important process as it prevents sensitive corporate or personal data from inadvertently ending up in the wrong hands. Just like the functions outlined in the other three phases of PC lifecycle management, this process should be automated and able to be managed remotely.

### **The Path to Effective PCLM**

Given the complexity and rate of change in today's IT environments, you can't simply buy technology, plug it into your existing infrastructure, and expect improvements to occur automatically.

Instead, you need to implement an automated approach that addresses the needs of both users and IT—one that can strike a fine balance between responsiveness and control. The key to achieving this balance is to carefully integrate your PC lifecycle management process with the right management tools. Establishing an integrated PCLM will enable you to:

- Accomplish more tasks with fewer resources.
- Measure, repeat, and report on your management activities.
- Decrease or eliminate task duplication.

Once your PCLM plan is in place, you'll finally be able to minimize costs, downtime, and risk while providing positive and timely responses to changing organizational needs.



**North America Headquarters**  
14100 Southwest Freeway  
Suite 400  
Sugar Land, Texas 77478  
Tel 713 316 4900  
Toll 866 722 5225  
Fax 713 316 4975

**International Headquarters**  
Gainsborough House  
2 Sheen Road  
Richmond Surrey TW91AE  
United Kingdom  
Tel +44 844 736 5214  
Fax +44 844 736 5894

**Scalable Software**  
9148 Bonita Beach Road  
Suite 210  
Bonita Springs, Florida 34135  
Tel 239 495 0541  
Fax 239 498 7344

**Web** [www.scalable.com](http://www.scalable.com)  
**E-Mail** [info@scalable.com](mailto:info@scalable.com)