

Standardized Systems Management

A White Paper by Nelson Ruest and Danielle Ruest

January 24, 2006

ABOUT SYMANTEC

Copyright © 2008 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, Altiris and any Altiris or Symantec trademarks used in the product 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.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

THE DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID. SYMANTEC CORPORATION, INCLUDING WITHOUT LIMITATION ITS AFFILIATES AND SUBSIDIARIES, SHALL NOT BE LIABLE FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES IN CONNECTION WITH THE FURNISHING, PERFORMANCE, OR USE OF THIS DOCUMENTATION. THE INFORMATION CONTAINED IN THIS DOCUMENTATION IS SUBJECT TO CHANGE WITHOUT NOTICE.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in Commercial Computer Software or Commercial Computer Software Documentation," as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display, or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
20330 Stevens Creek Blvd.
Cupertino, CA 95014
<http://www.symantec.com>

Altiris, Inc.
588 W. 400 S.
Lindon, UT 84042
<http://www.altiris.com>

CONTENTS

Abstract	ii
About the Authors	ii
IT Issues Today	1
Introducing Standardized Systems Management	3
IT is a Service	4
Using a Service Lifecycle	4
Understanding IT Business Goals	6
Using an SSM Model	8
Moving to Standardized Systems Management	9
Driving Principles of Quality IT Service	9
Principle No. 1	9
Principle No. 2	9
Principle No. 3	10
Principle No. 4	11
Principle No. 5	11
Principle No. 6	12
Principle No. 7	13
Principle No. 8	13
Principle No. 9	14
Principle No. 10	15
Principle No. 11	15
Principle No. 12	15
Principle No. 13	15
Principle No. 14	17
Principle No. 15	17
Implementing SSM	17
Quantifiable Business Outcomes	19
References	20
Bibliography	21

ABSTRACT

According to industry analysts Gartner Research, the difference in cost between an unmanaged and a well-managed computer system can be as much as 36 percent. This is significant, especially in times when budget cuts are much more the norm than budget increases. But how do you get from an unmanaged to a well-managed state? The answer: standardized processes that rely on automation to reduce potential diversity within deployed systems. This paper covers the “state of the union” for most organizations and helps identify why many are still in an unmanaged PC state. It then goes on to outline procedures and processes organizations can use to move to a well-managed state and obtain the corresponding cost reductions.

About the Authors

Danielle Ruest and Nelson Ruest are IT professionals specializing in systems administration, migration planning, software management and architecture design. They are authors of multiple books, notably two books published by McGraw-Hill Osborne, “Windows Server 2003: Best Practices for Enterprise Deployments”, ISBN 0-07-222343-X and “Windows Server 2003 Pocket Administrator”, ISBN 0-07-222977-2 as well as “Preparing for .NET Enterprise Technologies”, published by Addison Wesley, ISBN 0-201-73487-7. They have extensive experience in software packaging and managing large packaging projects. They are working on their fourth book, “Enterprise Software Packaging: Patterns and Practices,” to be released by year end.

IT ISSUES TODAY

According to Gartner Research, a well-managed system can help reduce total cost of operation (TCO) by up to 36 percent...

Organizations rely more and more on Information Technology (IT) services to get the job done. In fact, it would be hard to imagine anyone doing it any other way today. This means each organization must put in place, manage and administer an IT Infrastructure. In most cases, this focuses on the implementation and support of a *Distributed Environment*—a network supported by a series of centralized servers, optional data repositories such as mainframes or mini-computers and decentralized points of access to that network, usually in the form of personal computers, or rather, workstations and mobile systems.

For many organizations, this means using a variety of tools, possibly even a variety of operating systems. Even if you don't have to manage different operating systems, your organization might still be managing diversity in the form of different standards being applied to each component of the network. In other organizations, diversity is introduced through the use of heterogeneous operating systems. There may be sound justifications for the introduction and maintenance of heterogeneous systems, but the end result is the same: diversity. Managing diverse systems can only increase costs and reduce effectiveness because it is simply impossible to know everything about everything. When organizations use different systems, they cannot master them all unless they put in place and pay for different teams of professionals that will have the sole purpose of supporting one and only one of the systems in place. This level of support is obviously possible only for organizations that have the scope and size required to support the cost of this effort.

Standardizing on a single operating system is one of the ways organizations can reduce costs in IT, but not the only way. There is no doubt that replacing a variety of systems with a single unified OS is expensive and time-consuming, but the advantages are clear. Everyone works with the same tools and everyone uses the same approaches. What is even more important is going from a non-managed system to a managed system. Non-managed systems are computers that are deployed in an ad hoc manner, by different professionals using different procedures each time a new system is required. Managed systems refer to systems that use an automated, reproducible process each time a new system is required. Even if there is more than one operating system to support, using a managed system approach will greatly reduce costs because it directly addresses the issue of diversity.

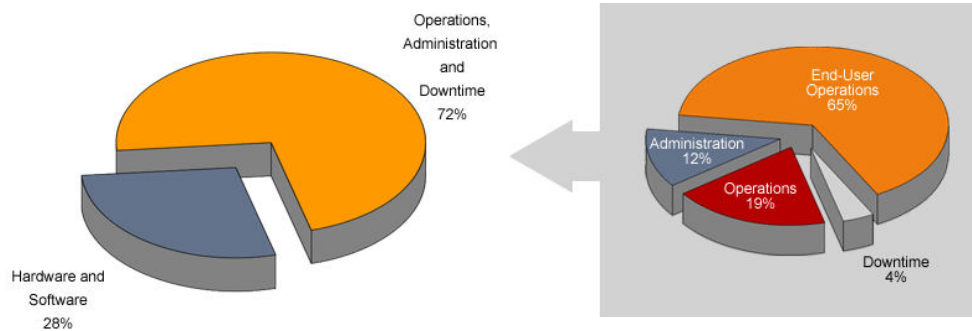
According to Gartner Research, only 28 percent of the total cost of ownership for unmanaged systems—in this case Windows XP systems—is composed of hardware and software acquisition costs (see Figure 1).

Of the remaining 72 percent, operations and downtime make up another 35 percent while the rest is composed of end user operations.

This means that the difference between a managed and an unmanaged system lies in cost savings focused on the 35 percent controlled by IT.

Figure 1

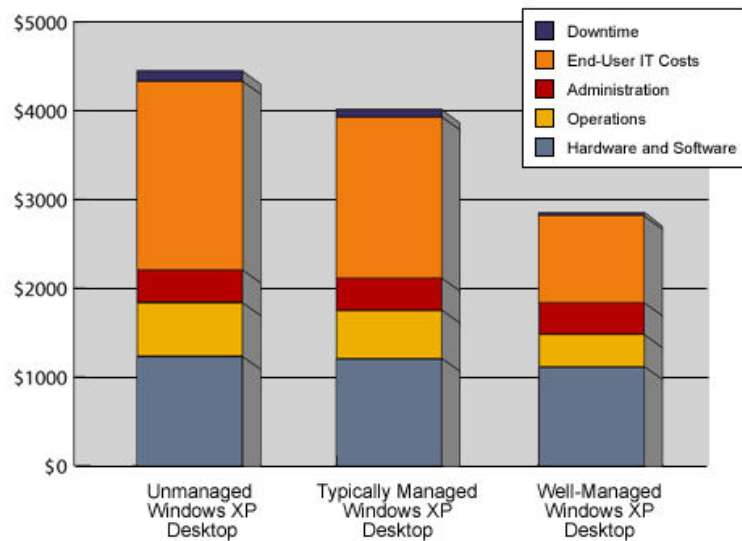
The cost of unmanaged systems.



In fact, Gartner Research claims that a well-managed system can reduce overall costs by 36 percent because well-managed systems even help reduce costs not normally associated with IT (see Figure 2).

Figure 2

Cost comparisons between unmanaged and managed systems. The total cost of owning a well-managed PC is 36 percent lower!



The question is: *How do you get from an unmanaged to a well-managed system?* This is the purpose of this paper—helping organizations of all sizes move from unmanaged to well-managed systems. It does so through the introduction of a simple concept: standardized systems management (SSM). SSM means implementing standardized processes that rely on automation to reduce potential diversity within deployed systems. SSM is implemented through the introduction of key concepts supported by standardized processes and procedures. This is the key to a well-managed system.

INTRODUCING STANDARDIZED SYSTEMS MANAGEMENT

Common Problems Due to Diversity

*The most common
problems due to running
non-standard systems
include:*

- 1. System diversity and
therefore, complexity*
- 2. Controlling costs*
- 3. Service quality*
- 4. Responsiveness to
both issues and new
requirements*

One of the major problems in organizations today is diversity. Users have a tendency to focus on the “personal” aspect of a PC, often insisting that they have the right to determine the tools that will be used on their “own” computer. But in fact, the PC must be viewed as a corporate *appliance*—a tool applied as a means to an end. Too many organizations rely on users or power users to provide support for their PC systems. PC support is not a user function, but an IT function. As such, IT is responsible for managing and maintaining all systems—even in small to medium shops. IT needs to focus on helping users perform their work according to the standards set by IT and corporate policies. The same applies to servers. Too many organizations still have servers on every floor or under staircases or wherever there is room. Servers must be protected and should be implicated in this effort to define IT standards and corporate policies. If anything, servers should even be addressed before PCs. This focus is the *first step* towards standardized systems management.

Standards are the key here. Organizations that run non-standard systems are faced with several potential issues on an ongoing basis. In fact, the common problems of non-standard IT services are well known today. The first is *complexity*. If systems and processes are not standardized, then organizations face support challenges. That’s because it is hard to determine where problems lie. In fact, in order to solve a problem, the person troubleshooting it must often reverse engineer the installation to identify what might have gone wrong. In addition, running non-standard systems means that it is impossible to automate their production since everyone has their own way of setting things up. Finally, change is very difficult to manage with non-standard systems because each change must be performed individually because each system uses a diverse configuration.

The second common problem relates to *controlling costs*. Software costs are difficult to control in these situations because acquisitions are often ad hoc and occur only when individuals indicate they need something. IT management and support costs soar since each service demand is an ad hoc demand and cannot be predicted with any degree of accuracy. End users also experience increased downtime because problems are unforeseen and take more time to resolve. This directly impacts organizational productivity and can have a negative impact on profitability or simply performance.

The third common problem non-standard systems engender relates to *quality of service*. In a non-standard environment, there is simply no such thing as service level agreements. It is understandable: how can you predict how well a service will run if you cannot state with determination how it was configured? This will also impact service availability since unforeseen problems can occur at any time. Finally, each time you make a change to the configuration of a service, you will

not be able to expect predictable outcomes since you cannot guarantee that you fully understand the operation of the service itself or its dependent components.

The fourth common problem is *responsiveness*. IT personnel have no time to move forward and proactively prepare services because they are constantly putting out fires. This reactive approach to IT service delivery is time-consuming and very hard on workers both in IT and in the end user community. IT is also challenged when it needs to deliver new services since all of their staff is overrun with reactive service demands. Finally, because most IT operations are based on manual processes—often manual processes without written guidance—it is impossible to expect standard results for given operations. Non-standard manual processes take more time because they often have to be re-invented each time the operation is performed.

Each of these common problems is directly related to the fact that IT is operating in a reactive instead of a proactive mode. In fact, if you are operating in this mode, you probably know best the types of problems you'd like to correct. The key to the elimination of these problems is to change this crucial aspect of IT service delivery.

IT is a Service

The Concise Oxford Dictionary defines the word service as among other things: "...work done to meet a general need, ...work done...on behalf of an employer, ...provision of what is necessary..."

If a definition of service is "...work done to meet a general need ... provision of what is necessary...", then IT is a service because information technology fulfills a key set of needs for organizations—services that support the business functions of the organization's user-base. It is no wonder that one of the key elements of a network is the *server*. This machine offers a clear set of *services* to the IT community. But machines are not the only element providing services to user communities; IT professionals also provide services and, as in every service profession, should provide high-quality services.

Because IT is a service, it must be bound by a clear set of rules that take into account what a service truly is and especially, how a service can be a success. Face it: if your IT service doesn't respond to business needs, it will directly impact the productivity of your organization.

Using a Service Lifecycle

The *second step* in the implementation of a standardized systems management approach lies in adopting a lifecycle management approach to all systems—servers and PCs. To do so, you need to rely on the use of an IT service model. Traditional IT service models abound in the

The Phases of the Service Lifecycle Management Model

The lifecycle includes four phases:

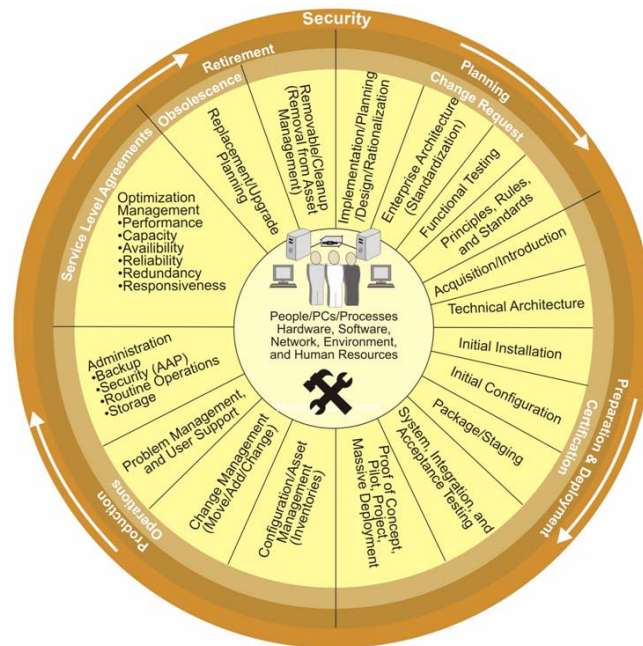
1. *Planning*
2. *Preparation and Deployment*
3. *Production*
4. *Retirement*

industry, but one that seems to work well identifies four phases for Service Lifecycle Management:

1. **Planning**—Focuses on identifying and preparing solutions for deployment.
2. **Preparation and deployment**—Focuses on acquiring, packaging, configuring, installing, and testing deployment strategies for approved solutions.
3. **Production**—Focuses on problem and change management, service optimization, and general service administration within the production network.
4. **Retirement**—Focuses on replacement or upgrade planning and removal of obsolete technologies and processes.

The Service Lifecycle Management model with its four phases is illustrated in Figure 3. Note its cyclical nature and the repeatable processes that emerge from this model. Each service should run through each phase of this lifecycle.

Figure 3
The Service Lifecycle Management model.



Of special note is the security element—it surrounds the entire lifecycle and must be considered at each phase of service delivery. Another key element of this model is the interaction of people, processes and technology, which is at the core of the entire lifecycle.

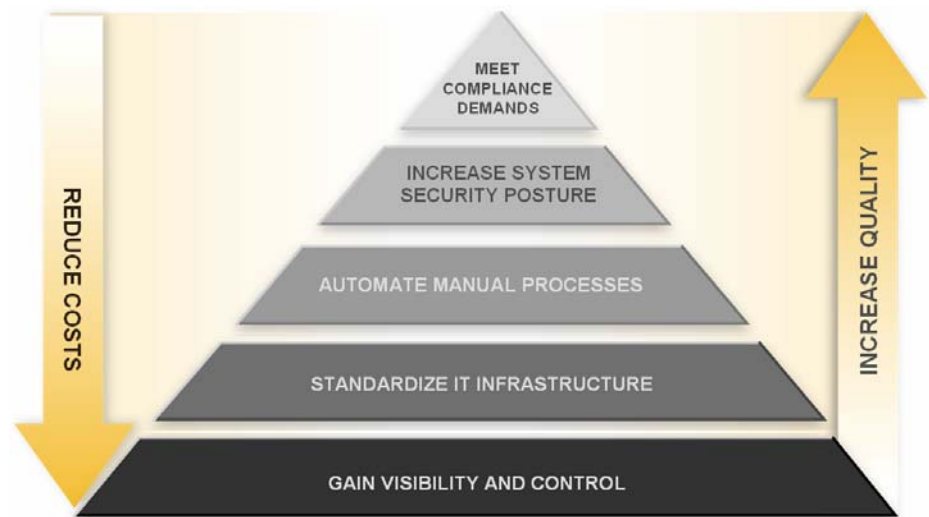
Using such a service model will allow your IT team to understand the cyclical nature of service deployment and will provide a more holistic view to the entire network service framework.

Understanding IT Business Goals

If IT is a service and provides services based on a service lifecycle model, then it needs to understand the business goals that drive it. Learning that IT also has business goals that fit within the overall organizational goals is the *third step* towards implementing standardized systems management. Figure 4 outlines a model for the definition of IT's business goals.

Figure 4

A framework for the definition of IT business goals.



IT business goals are typically focused on supporting corporate initiatives. To support corporate initiatives organizations should focus on increasing the quality of IT services, while reducing the cost associated with delivering the services. With the proliferation of new regulations, most IT organizations are trying to meet compliance demands for regulations such as Sarbanes-Oxley, HIPAA, FISMA, PCI, Base II, etc. A majority of the regulations and governance activities focus on ensuring system security. This is the end goal for IT.

To achieve this goal, IT needs to begin with the basics: gain visibility and control over what it needs to manage. It is simply amazing that despite the proliferation of free and commercial tools for the automatic enumeration of the contents of a network, that so many organizations still have no idea what is in their technological inventory. Generating inventory data can be as easy as writing a script to collect it, using a vulnerability scanning tool to identify what is on each computer system or even implementing an inventory control or asset management solution. *There is no justification for not having access to inventory data today.*

Once you are aware of what needs to be managed, you can begin the elaboration of standards for both the way IT operates and for the technologies that IT implements. One key area here is the Standard Operating Procedure (SOP). SOPs do not have to be rigid procedures

that never change; they need to be standard approaches to specific operations. Once you have a standard in place, then you can work on making it evolve as your infrastructure needs change.¹

Then, once your standards are in place, you can begin to automate processes. Standard processes are a lot easier to automate because they are repeatable and predictable. Automation should include processes such as PC or server build and deployment, application deployment, patch and service pack application, as well as system monitoring and alert generation.

Once automation is in place, you can put more emphasis on securing the entire infrastructure. This is not to say that security has not been a consideration up until now, but rather to say that once systems are under control, you have more free time to proactively ensure all systems are secure at all times. This will be a stepping stone towards the final goal: compliance management. In addition, IT needs to ensure that costs are controlled and that quality is a major aspect of every service delivery.

As you can see, the most significant amount of work related to implementing standardized systems management lies within the first three business goals for IT: identifying what you have, implementing standards and automating processes. Once again, Gartner Research provides insight into these aspects and the level of maturity your IT infrastructure has. Figure 5 illustrates this model.

	Basic Uncoordinated infrastructure	Centralized Infrastructure centralization	Standardized Standard resources, configurations	Rationalized Consolidate to fewer	Virtualized Infrastructure resources pooled	Service-Based Services managed holistically	Policy-Based Dynamic optimization to meet SLAs
Objective	React	Manage	Reduce complexity	Economies of scale	Flexibility, reduce costs	Service-level delivery	Business agility
Ability to Change	Weeks to months	Weeks to months	Weeks	Days to weeks	Minutes to weeks	Minutes	Seconds to minutes
Pricing Scheme	Ad hoc	Fixed costs	Reduced, fixed costs	Reduced, fixed costs	Shared costs	Variable usage costs	Variable business costs
Business Interface	No SLAs	Arbitrary SLAs	Class-of-service SLAs	Class-of-service SLAs	Flexible SLAs	End-to-end SLAs	Business SLAs
Resource Utilization	Unknown	Known, poor	Reallocation	Rationalized	Shared pools	Service-based pools	Policy-based sharing
Organization	Distributed	Centralized	Shared	Consolidated	Pooled ownership	Service-oriented	Business-oriented
Processes and Automation	Ad hoc	Defined processes, monitoring	Life cycle standards management	Mature processes	Capacity management, dynamic sharing	End-to-end service management	Policy management

Source: Gartner

In this model, Gartner Research has identified seven stages of infrastructure maturity. When explaining the model, Gartner Research states: “These stages are not necessarily sequential, and an organization might find out that they are in several stages at the same time. However, the stages represent the most efficient steps to evolve towards a real-time infrastructure. For example, it is much easier to virtualize an infrastructure once the infrastructure is standardized—with full life cycle standards already in place.”²

Figure 5
The Gartner Research IT infrastructure maturity model.

According to Gartner, roughly 60 percent of Fortune 500 organizations—and a much higher percentage of smaller companies—are in the first two stages or in the Basic or Centralized stages, while 90 percent have evolved no further than the first three stages of evolution. This is one key reason why the first place to start is to focus on standardization and automation.

Using an SSM Model

The final and *fourth step* towards implementing standardized systems management is to use an SSM model. Because you now know that standardization and automation are key factors of SSM, it makes sense to expect that they would form part of the framework. In fact, they will be supplemented with a third pillar: maintenance. Maintenance will be critical to the proper management of the SSM once it is in place. Figure 6 illustrates the new SSM pyramid.

Figure 6
Using an SSM model.



This model relies on three pillars: standardization, automation and maintenance. Standardization will serve to reduce diversity mostly in server and desktop configurations. Since there are many more desktops than servers, this is often the best place to start. Automation will focus on the reduction of manual, labor-intensive processes. Once again, the best place to start is in desktop deployment and desktop configuration management. Finally, maintenance will focus on the implementation of structured change management processes to ensure the stability of the solutions you put in place. Each and every one of these elements should be covered by documented IT policies and procedures.

MOVING TO STANDARDIZED SYSTEMS MANAGEMENT

There are several activities involved in moving towards a standardized systems management structure within IT and as you would expect, few are easy. IT organizations that are at the first three stages of the Gartner Maturity Model (see Figure 5 above) are faced with many challenges when trying to move to SSM. Many have heterogeneous systems in place and may even have heterogeneous operating systems. Others will be involved in mergers and/or acquisitions which will add significant challenges as they try to make their systems work together. Internal politics are also a factor as departmental heads will prefer to continue running things “their way.” End users will tend to focus on the “personal” in personal computer and claim they have rights to their particular machine. IT itself will also offer some resistance as people are unwilling to change old habits. Finally, IT budgets will have an impact as they tend to become flatter and IT is tasked with “doing more with less.”

But, despite these challenges, it is possible to move towards SSM and begin the long ride towards full IT maturity. One of the best ways to approach an SSM model is to define guiding principles for IT and share them with other members of the organization.

Driving Principles of Quality IT Service

The guiding principles IT implements will control the approaches used for change management within IT. They should be all encompassing and affect every level of the organization and every aspect of IT: technological and human. The best way to implement these approaches is often with the implementation of new technologies. For example, the deployment of Windows XP and or Vista is significant enough that it can support the implementation of an SSM framework. But, if you have already deployed XP, you can initiate internal processes that help you get ready for your next major deployment and apply these processes today to begin reaping the benefits they incur.

The following principles are examples of the types you might implement in your own organization.

Principle No. 1

All IT systems are corporate systems.

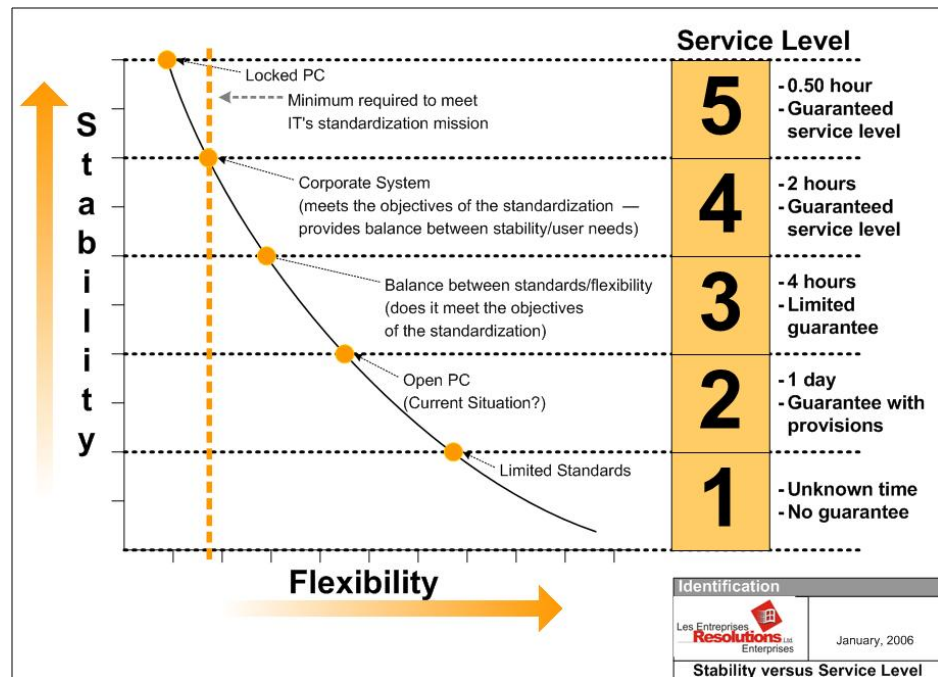
This means that PCs and other IT tools belong to the organization and not to individuals. Users have the right to personalize some elements of their PCs, but these are logical, not physical. Standards must be put in place at all IT service levels in order to ensure a measure of control and thus stability for all systems.

Principle No. 2

Lock down all computer systems.

IT must define the service levels it can offer to its user base. These service levels must be based on stability and robustness. The higher the stability, the better the guarantee of service IT can provide. If you take the example of a PC workstation, the more the environment is locked down, the greater its stability. The more it is flexible, the lesser its stability. This is illustrated in Figure 7. Stability and flexibility have a direct impact on the service levels an IT department can guarantee for all PCs.

Figure 7
Stability versus service level.



Many organizations today are at level 2 in this diagram since they either use PC operating systems that do not support the implementation of stability or allow all users to have administrative access to their PC. The goal of most organizations should be to aim for level 4. This level ensures a given stability but enough flexibility to allow for ease of evolution.

Principle No. 3

Follow industry standards in regards to acquisition, use and administration of IT infrastructures.

All organizations should put in place and manage their IT services according to the precepts of the IT industry if they want to implement systems that support business competitiveness. Several industry organizations provide guidelines for IT implementations. One of the most pertinent is the IT Infrastructure Library (ITIL). While your organization may not need to implement the rigid structure recommended by ITIL, you

may want to use ITIL as a source of guidance and additional information. ITIL can be found at http://www.itil.org/itil_e/index_e.html.

Principle No. 4

Centralize corporate systems whenever possible.

This does not mean that organizations that use decentralized administration structures must change. It means that in a client/server infrastructure as much as possible should be centralized on the server, especially for corporate systems. Servers are easier to update and upgrade than workstations. One good example is the use of Windows Terminal Services in application mode. This provides an excellent way to centralize applications and minimize update processes.

Using de-centralized applications means distributing the location of the system's executable code. Placing this code on PCs means being willing to support a more complex update process. In some cases though, this may be the only approach that meets your business needs. A good example of this is office productivity tools, especially for mobile users—each user needs to have dedicated access to these tools in support of their work.

Principle No. 5

Rationalize all product selection within the organization.

Rationalization of all products and technologies in use in the organization is one of the key pillars of standardization. It is impossible to standardize on 2,000 software products. Rationalizing means that the organization is responsible for the selection of all software and hardware tools, not individual users. Of course, your organizations can and should have a product recommendation procedure because even if it is not a user's role to select products, this doesn't mean they can't have good ideas.

When you rationalize products, you need to focus on a few key aspects of product selection. First, you should get rid of multiple versions of the same product. Running several versions of Microsoft Office, for example, is non-productive because of potential incompatibilities between document formats and the need to provide support on more than one version. Second, you should get rid of products that provide duplicate functions. For example, using two or three products for Web site editing may be practical for the Web editor, but very impractical for IT since it needs to prepare several products for deployment and then maintain them once deployed. The organization needs to put its foot down and provide stringent guidelines for product selection and approval. A good idea is to introduce a charge back scheme for any unofficial product. If a department is responsible for paying for product acquisition, deployment

Software Virtualization

Software virtualization is a new technology that provides support for multiple versions of the same product. While this is not a justification for avoiding rationalization of products, it is an excellent solution for situations where multiple versions of the same product must be run. For more information about software virtualization, visit <http://www.altiris.com/products/svs/>.

and maintenance because the product is not in the official portfolio, then they may rethink their approach.

A specific IT role should be put in place for tool selection. In addition, it is an excellent idea to create the position of Product Sponsor, or someone—usually a power user of the product—who is responsible for the evolution of the product in the network, identifying when patches or service packs are required for the product, and evaluating upgrade possibilities when new versions are released by the manufacturer.

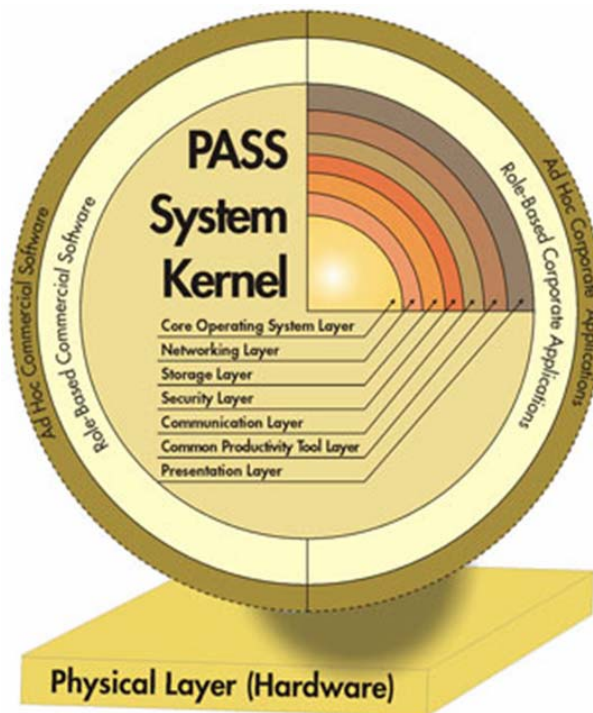
Principle No. 6

Standardize all configurations.

Every system construction process should be standardized. The best way to do this is to use a standard system construction model. The best way to do this is to use a standard system construction model. One such model is the Point of Access to Secure Services (PASS). The PASS model is illustrated in Figure 8. The PASS model³ provides a logical structure for the construction of corporate computer systems. It applies to both servers and workstations. In the case of the latter, role-based configurations focus on user roles; with servers, they focus on machine roles.

Figure 8

The PASS system construction model.



This model is based on the construction of a computer system that responds to corporate needs in three ways:

- The PASS system “kernel” is designed to meet the needs of the average corporate user. It contains all of the software components required to perform basic office automation and collaboration tasks. This includes all software for which you have a corporate license, all software that is royalty-free and required by all personnel, as well as the basic operating system. The system kernel is divided into a series of layers similar to the OSI Networking Model. In fact like the OSI Model, it uses seven layers to provide core corporate services. Because its functionalities are required by all personnel or all servers, this kernel is installed on all computer systems.
- Role-based applications and software are added on top of the kernel to meet the requirements of special IT roles everyone plays within the organization. Corporate applications are in-house programs that meet mission-critical or mission-support functions. Software is identified as role-based if not required by all personnel, but only for specific roles or tasks.
- Finally, an ad-hoc layer responds to highly specialized IT requirements that are often expressed on an individual basis. This ad-hoc layer can contain either software or applications.

To complete the picture, this logical model is based on standardized hardware within the organization. Standardized hardware simplifies the construction of PASS systems because they provide few variations in required configurations.

Principle No. 7

Use standard operating procedures.

As mentioned previously, standard operating procedures are the key to controlling change in your organization. If your IT personnel use SOPs, then you can predict results because everyone is using the same process to perform an activity. This reduces the opportunity for errors and simplifies system administration and maintenance.

Principle No. 8

Automate processes as much as possible.

Because you use standard operating procedures, you can identify specific areas where automation can provide assistance to IT processes. Some key areas for automation include:

- Inventory gathering and reporting
- System construction
- Application or software packaging
- Application or software deployment

- System monitoring and error correction

Automating these elements will help reduce operations and maintenance efforts for the IT team.

Principle No. 9

Implement a change management system.

The key to maintaining standards once they are in place is to control change as it is applied to them. A sound change management system lets you track each change as it is performed, simplifying the resolution of problems when they occur. Since everything is documented, it is much easier for IT organizations to determine the root causes of problems and provide much more rapid resolutions to issues.

Some of the immediate benefits you can draw from the implementation of a change management system include:

- Provide standardized approach to managing change
- Understand and minimize risks associated with change
- Ensure business continuity and support of corporate objectives
- Typically initiated by problem management process or by a project
- Often executed through release management
- A global reduction in the number of unapproved changes
- Change auditing

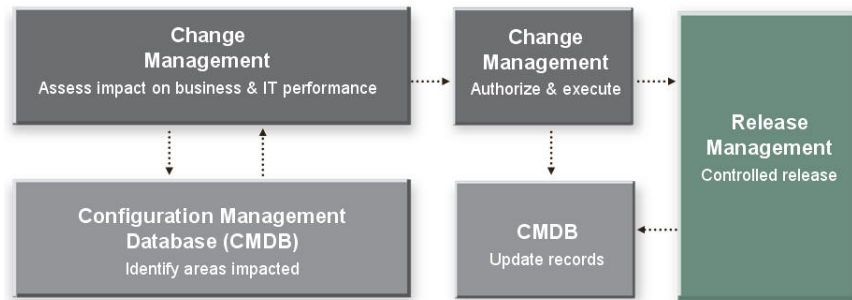
The foundation of managing change is the Configuration Management Database (CMDB) because it contains a complete record of all configuration items potentially affected by a change. To assess the potential impact of a change, the Request For Change (RFC) should be analyzed through an approval process. Whether the organization has a defined Change Advisory Board (CAB) or a dedicated change manager, it is imperative change approvals be included in the change process. This helps to ensure a successful change and assigns accountability. Throughout the change process, the CMDB is consistently updated to keep a constant, documented record of the entire IT environment. Having and maintaining a CMDB is also extremely important for supporting regulation compliance. The relationship between the CMDB and the change management process is illustrated in Figure 9.

“IT change management is the process that an enterprise uses to track modifications of any part of its IT infrastructure and application environment in a controlled manner, enabling and verifying approved changes with minimum disruption to the IT service.”

—Gartner Research

Figure 9

The relationship of change management with the CMDB.



Principle No. 10

Be prepared for network evolution.

Once the network has been standardized, IT must put in place specific processes for the constant update of the systems it contains. Patch management⁴, for example, is now a fact of life and must be regularly scheduled and performed. If your system design models include the ability to maintain and update them, then you will control how change is applied to your systems and be prepared for any eventuality. This approach will support a controlled, yet constant network evolution.

Principle No. 11

IT is the single point of service.

Every request that concerns any field covered by IT services must be directed to the IT department. It cannot be addressed by any other part of the organization. One of the most common problems non-standardized IT organizations face is the fulfillment of IT requests by other departments. Ensuring that IT is the single point of service eliminates the potential disruption of having multiple departments responding to IT needs in different ways.

Principle No. 12

Form a specific service contract between IT and the user base.

The objective of IT is to put in place effective services that respond to organizational needs. The service contract between IT and its user base must be clearly defined and leave no room for ambiguity. In order to avoid ambiguity, IT needs to clearly define all of the terms that will be used in the service contract. A simple form for this service contract can be a list that includes all of the services provided by IT and expected service levels for each. IT should then use Principle 2 to broadcast this message.

Principle No. 13

Define a common vocabulary.

IT needs to use terms that are clear and if possible, concise when defining the service contract. In order to do this, it is often important for IT to remove themselves from their own situation and take a global view of their role within the organization. Sample common terms are included here:

- *Empowered user*—This is a term that is often misunderstood as much by IT as by users. An empowered user is an autonomous user, not a self-service user. The user should never be a computer technician. It is not a user's role to repair a PC or install PC software. *IT should provide powerful tools whose functions are to assist users in the accomplishment of their tasks.* Empowered user means that the user can perform their tasks without any obstruction or interruption.
- *Roles within the service contract*—At least three roles need to be defined:
 - IT is a service provider. Its role is to provide advisory and leadership services (related to technological use) to the user base.
 - The IT service desk is the user base's single point of contact with IT. All user requests should go through the IT service desk.
 - The user is an IT customer that has specific needs. These needs must fit within the corporate IT structure.

These roles help shape the relationships IT must manage. IT must respond to the demands of its customers as a whole. User requests are no longer treated on an individual basis with individual solutions, but rather within the context of a global IT strategy.

- *A service policy*—Given clear role definitions, IT can begin to define a service policy. This policy must cover the following elements:
 - Empowering the user means allowing them to perform work without interruption of service.
 - One of IT's roles is to help define the needs of its user base and recommend solutions.
 - IT must form a business partnership with its client departments.
 - As a service provider, IT must provide quality tools and services to its customer base.

Principle No. 14

Implement complete and interactive communications processes.

IT should be transparent and provide complete information to all levels of the organization at all times. Thus a continuous communications process should be in place. People should not learn of critical aspects of a project or of an IT implementation at the last minute. One good place to start is with an information collection—collecting key information from various business units to ensure IT understands their needs.

This communications process must also involve training and communications resources, as well as user and management representatives.

Principle No. 15

Implement a virtual computing environment.

Every user should be able to use any point of access (or workstation) in the corporate network and be able to be immediately productive. This principle is based on the use of standard system construction models which provide the same base set of services to every user. Since all systems provide one single set of services, any user can access any of these services from any system. In addition, if users require access to custom services, they can use technologies such as Windows' Remote Desktop to access their own personal computer from any location in the organization. Using the Remote Desktop, they have access to any and every application installed on their system.

Implementing SSM

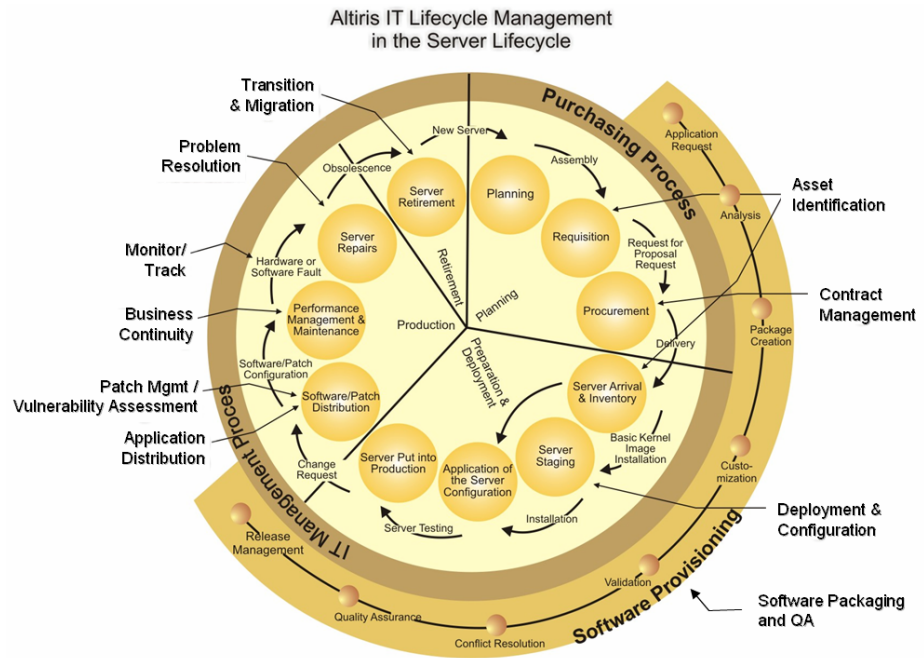
Using the principles outlined above, you can begin to implement standardized systems management. Remember that the implementation of SSM is based on three key pillars: standardization, automation and maintenance. Begin by outlining your initial standards, find opportunities for automation and implement structured change management to control system maintenance.

One of the best ways to make this move is to select a systems management solution—a solution that addresses the complete service lifecycle as defined in Figure 3 earlier in this document. Such solutions provide complete support for the principles outlined here and also help immensely in the automation of standard processes. Ideally, the tool you select will be based on industry best practices and will incorporate standard management principles within its core operations model.

Altiris® Total Management Suite™ offers a complete set of tools that control the entire system lifecycle. Figure 10 illustrates how the Altiris solution helps address each and every phase of standardized system management.

Figure 10

The Altiris system lifecycle management.



As with service lifecycles, system lifecycles include four key phases: Purchasing or Acquisition, Preparation and Deployment, Maintenance, and Retirement. As you can see, Altiris Total Management Suite, which includes Wise Package Studio integrated software packaging environment help address each one of these phases for client systems. While this illustration focuses on server provisioning, the Altiris toolkit provides the same set of functionalities for client systems, be they PCs, mobile systems or even personal digital assistants (PDA).

QUANTIFIABLE BUSINESS OUTCOMES

The purpose of SSM is to provide direct returns on investment (ROI) to organizations that implement it. When you choose to move forward with this strategy, you will find that you will now be able to quantify the benefits you will draw from SSM. In fact, you can expect that the implementation of SSM will provide you with the following capabilities:

- Standardized desktop configuration
- Standardized server operations
- Elimination of software conflicts through application standardization
- Reduction of the risks associated with desktop and server changes
- Increase in the effectiveness of existing resources through controlled automation
- Reduced desktop downtime through automated state maintenance
- Automated software installation procedures
- The ability to meet SLAs and reduce operational costs
- Reduced deployment failures
- Improved quality of service
- Reduced hardware and software support costs
- Increased understanding of IT assets and increased accountability
- Use of a centralized CMDB to reduce the risk associated with change
- Increased IT infrastructure ROI and ability to develop accurate budgets
- Reduced costs and complexity associated with the maintenance of multiple integration points
- Strong potential for server consolidation
- Consolidated software license agreements

Each and every one of these capabilities will help reduce your operating overhead and provide a better quality of service to your user community. After all, the primary purpose of IT is to provide quality services to the user base.

REFERENCES

¹ For more information about SOPs, see “Appendix B: Designing Standard Operating Procedures” in *The Case for Quality Assurance in Enterprise*.

² For more information about Software Packaging, visit http://www.wise.com/library/Quality_White_Paper.pdf.

³ The PASS model is an original concept of Resolutions Enterprises Ltd. For more information about the PASS model, see “Enterprise Software Packaging Practices, Benefits and Strategic Advantages” at <http://www.wise.com/esp/espwhitepaper.pdf>.

⁴ For more information about patch management principles, see “A Practical Guide for Patch Testing” at http://www.wise.com/library/Patch_Whitepaper.pdf.

BIBLIOGRAPHY

Automated Software Distribution Does Not Reduce Staff. R. Colville. Gartner Advisory. 30 November 2001.

Desktop Software Configuration: Key to Desktop Availability. R. Colville and D. Scott. Gartner Advisory. 28 June 2001.

Preparing for .NET Enterprise Technologies. Nelson Ruest and Danielle Ruest. Addison-Wesley. ISBN: 0-201-73487-7.

Optimize Change and Configuration Management With People, Process and Tools. Ronni Colville, Patricia Adams and Kris Brittain. Gartner Research, 3 August 2005.