Microsoft

Optimizing IT Infrastructures

Using Best Practices to Drive Down PC Labor Costs

Abstract

Deployment and management costs of PCs and the infrastructure that supports them use up 30 to 45 percent of most organizations' IT budget. However, increasingly complex IT environments often incur increased costs and require service level compromises. This paper presents the results of surveys and analysis conducted during 2005 at 14 private enterprises. These organizations used best practices and management software technologies to optimize their organization's IT infrastructure and reduce PC management costs.

Results of this study indicate a direct correlation between the number of best practices adopted, the management technologies used, and the positive impact on reducing PC-related labor costs. Technical decision makers, especially those responsible for desktop PC environments, will gain insight into how they can better manage their IT environment with fewer financial resources.

April 2006

William Barna, MBA
Senior Program Manager
Windows Enterprise Management Division

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft or its respective suppliers cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. MICROSOFT AND ITS RESPECTIVE SUPPLIERS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

© 2006 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, .NET, Windows, Windows NT and the Windows logo, are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Microsoft Corporation • One Microsoft Way • Redmond, WA 98052-6399 • USA

Contents

Executive Summary

Every CIO is under pressure to reduce costs and improve delivered services. Because PCs and their supporting infrastructures often represent 30 to 45 percent of an IT budget and are users' point of contact to their organization's IT department, reducing costs while improving service levels is a high priority.[1]

According to Gartner, a typically managed PC costs a 2,500-user organization in the United States between $4,618 and $5,024 per year. Approximately 13 percent of this amount relates to IT labor.[2] Therefore, IT labor is a logical place to reduce costs because it directly affects the IT budget and can be reduced by improving IT processes or adopting best practices.

This white paper summarizes the results of independent research conducted during 2005 at 31 government, educational, and private sector organizations in the United States. The analysis compares best practice adoption rates to IT labor costs and links those costs to management software technologies used at these organizations. This information can be used to develop cost reduction strategies at virtually any organization.

An organization's IT labor costs are determined by its:

- **Level of IT infrastructure optimization,** which contributes 54 percent of IT costs.
- **Industry,** which contributes 34 percent of IT costs.
- **Size,** which contributes 12 percent of IT costs.

However, when costs are analyzed by using all three of these factors simultaneously, it is difficult to isolate the contribution of optimized infrastructures alone. To reduce the effects of an organization's industry, the metrics provided in this paper are limited to 14 private enterprise organizations. A similar analysis was performed for the study's government and educational organizations. It yielded the same relationship between IT labor costs and best practices as the analysis of enterprise organizations. Metrics from all 31 organizations are provided only to demonstrate the cost effects of an organization's industry.

Throughout this paper, organizations are categorized into three levels of infrastructure optimization, which reflect the number of best practices that the organizations have adopted. The six best practices used in this paper were chosen from a group of 21 best practices selected during research in 2005. Adoption of these best practices, which collectively account for $226 per PC annual savings, represent 44 percent of the potential savings of moving from the lowest to the highest infrastructure optimization level. Organizations that used two or fewer best practices were categorized as having Basic infrastructure optimization. Adopting three or four best practices qualified organizations as Standardized, and adopting five or six best practices was equivalent to a Rationalized level of infrastructure optimization.

Study results show that:

- **Organizations can reduce annual IT labor costs by improving their infrastructure optimization levels.**
  - Moving from Basic to Standardized optimization reduces IT costs by $233 per PC.
  - Moving from Standardized to Rationalized optimization reduces IT costs by $280 per PC.
  - The total savings of moving from Basic to Rationalized optimization can reduce IT costs by $513 per PC.
- **Organizations can also reduce annual IT labor costs by up to $226 per PC by adopting best practices.**
  - Standardizing on a single desktop operating system reduces costs by $52 per PC.
  - Ensuring that users install only software sanctioned by their IT department reduces costs by $50 per PC.

[1] Data from the GCR Custom Research survey of 150 IT professionals conducted in August 2005. Costs include PC hardware, PC software, PC labor, service desk, and supporting server infrastructure.

[2] Silver, Michael and Troni, Federica, "Using Best Practices to Reduce Desktop PC TCO, 2005-2006 Update", December 2005, RN G00135328, Gartner.

- Managing PC firewalls with a centralized, comprehensive security program reduces costs by $39 per PC.
- Ensuring that users can change only PC settings that do not jeopardize reliability or security reduces costs by $30 per PC.
- Automating password resets so that users can reset their passwords without IT assistance reduces costs by $29 per PC.
- Automating software distribution methods that use policies to install PC applications and security updates remotely reduces costs by $26 per PC.

- **Microsoft management software increased best practice adoption rates and reduced annual PC labor costs.**
  - Using the Microsoft Windows Active Directory® service and Group Policies helped to reduce costs by $171 per PC.
  - Using both Active Directory and Microsoft System Management Server (SMS) helped to reduce IT costs by $199 per PC.
- **Different infrastructure optimization levels require different IT labor cost reduction strategies.**
  - Organizations at the Basic level should implement a PC strategy that minimizes the number of operating systems and should deploy a directory service with centralized policies to attain a managed desktop.
  - Organizations at the Standardized level should manage their PCs tightly with policies and extend management capabilities with systems management software.
  - Organizations at the Rationalized level should look to other sources of information for operational improvements because they have already accomplished the recommendations in this paper.
  - Regardless of their infrastructure optimization level, all organizations should develop a roadmap for adopting new PC operating systems and management software.

Introduction

Every CIO is under pressure to reduce costs and increase service levels. According to Gartner, a typically managed PC costs a 2,500-user organization in the United States between $4,618 and $5,024 per year. Approximately thirteen percent of this amount relates to IT labor.[2]

Reducing IT labor costs is an effective way to reduce IT costs because labor costs affect the IT budget directly and can be reduced by adopting best practices. This paper describes the role that management software technology played in reducing costs and analyzes how 14 private enterprises reduced their IT labor costs by optimizing their IT infrastructure with best practices.

Study results show how organizations at the Basic and Standardized levels of infrastructure optimization can reduce costs by:

- Implementing some or all of the six best practices profiled in this study.
- Using the Microsoft Windows Active Directory service, Group Policies, and SMS to implement these best practices.

This paper describes IT labor spending trends at 14 private enterprise companies and compares best practice adoption, supporting technologies, and their impact on IT labor costs. Infrastructure optimization and best practices are presented as vendor-neutral IT processes and technologies, although Microsoft technologies are highlighted for the purposes of this paper. When comparing competing technologies, organizations should consider the cost of delivering and maintaining best practices with each vendor's products. In general, integrated solutions such as the Active Directory service and SMS will be less complex and therefore less expensive to deploy and operate.

Infrastructure Optimization

Results of this study show that an organization's level of infrastructure optimization is the strongest driver of IT labor costs. Infrastructure optimization focuses on the overall development of an organization's IT processes and the specific technologies that the organization adopts. Microsoft developed its Infrastructure Optimization Model (IOM) to help organizations measure the sophistication of their current IT processes and technology investments and to prioritize future IT investments. Exhibit 1 illustrates the characteristics of organizations at each IOM level.

IOM Level	IOM Level Descriptions[3]
Basic	▪ Most IT resources are used to keep IT functioning with reactive management. ▪ Systems are complex, incompatible, and expensive and do not provide services throughout the organization. ▪ Organizations use few IT policies and automated processes.
Standardized	▪ Organizations run somewhat effective, centralized IT departments. ▪ IT systems remain complex, incompatible, and expensive and are run as standalone operations. ▪ Basic automation is provided by a centralized IT group; pockets of automated services exist at business units.
Rationalized	▪ Long-term IT strategy is developed jointly by business and IT groups. ▪ IT policies are defined with business criteria and enforced with IT processes and technology. ▪ Complexity is engineered out of IT processes, and application compatibility issues are minimal. ▪ This is the most cost-effective infrastructure optimization state.
Dynamic	▪ Cost savings are secondary to maximizing business agility, which is a source of competitive advantage. ▪ Some decision making is decentralized to bring decisions closer to business processes. ▪ IT systems are highly automated, flexible, and respond quickly to changing business conditions. ▪ Organizations may choose not to implement certain IT best practices because they reduce business agility.

Exhibit 1: Characteristics of organizations at different levels of infrastructure optimization

[3] For a complete description of the IOM, see Appendix B, "Infrastructure Optimization."

Although Exhibit 1 describes the Dynamic level of infrastructure optimization, none of the organizations participating in this study demonstrated this advanced level of IT process development.

Best Practices

Best practices are IT processes designed to minimize costs or improve service levels or business agility. Because the research in this paper pre-dates the Microsoft IOM, this study uses the number of best practices each organization follows as an indicator of infrastructure optimization. The 14 private enterprises participating in this study were surveyed for their staffing levels, management technologies used, and best practice adoption rate. Of the 21 best practices collected, six had strong relationships with lower IT labor costs. Exhibit 2 describes these best practices.

Best Practice	Best Practice Description
Standardize on a single operating system.	Organizations that standardized on a single desktop operating system saved IT labor costs compared to organizations that ran more than one operating system.
Users can install only software sanctioned by IT.	Authorized software is delivered automatically through policy-based management. Users may only install software that is advertised by IT groups in management software or a directory.
Centrally managed PC firewall	Organizations with a centrally managed PC firewall can limit the ports on which PCs can send and receive traffic. Ports can be opened or closed in response to new security threats.
Users can only change PC settings that do not compromise reliability or security.	IT groups determine which PC settings are critical for reliability and security and use software policies to prevent unauthorized users from making changes. Examples include changes to the Windows registry and firewall settings.
Automated password reset	Users can reset their passwords without assistance from the service desk.
Automated software distribution	PC applications and patches are deployed by automated tools based on group membership.

Exhibit 2: Best practices presented in this study

Value, TCO, and IT Labor Costs

This paper shows the effects of various drivers such as infrastructure optimization on IT labor costs associated with managing a desktop environment. IT labor costs are a category of total cost of ownership (TCO), which in turn is part of the total business value of any software technology. Exhibit 3 illustrates these relationships.

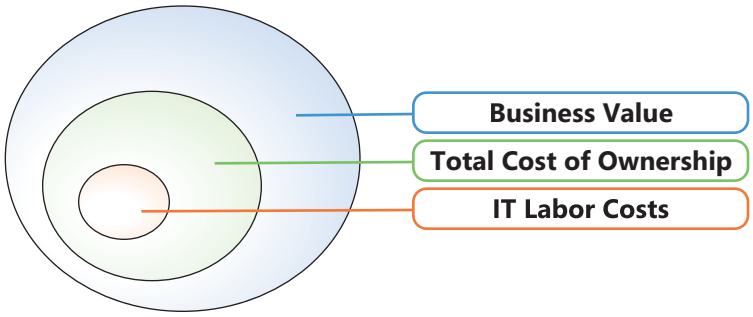


Exhibit 3: Relationships of business value, TCO, and IT labor costs

Analyst firms, consulting firms, and vendors that evaluate PC costs use many TCO models. In general these models, which are very similar, all include direct and indirect cost components. Hardware, software, and IT staffing are direct costs; they are included in the IT budget and can be planned for. Indirect costs on the other hand, occur outside the IT organization. Organizations experience these costs as a loss of employee productivity. For example, indirect costs are incurred by troubleshooting a PC before calling the service desk, installing software, backing up data, or attending formal or informal training.

Exhibit 4 illustrates the cost categories of the annual TCO cost profile of $4,500 per PC. TCO is measured for a Windows-based PC operating in a typically managed IT environment.

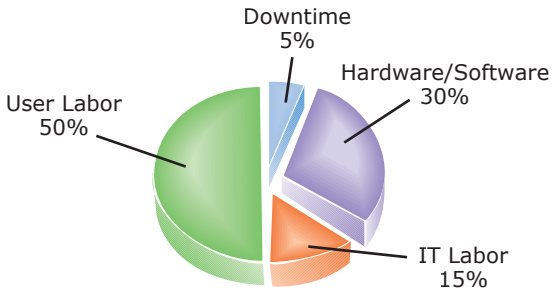


Exhibit 4: TCO of Windows PCs by cost category

Exhibit 5 describes the distribution of these costs for an organization spending $4,500 per PC per year. As infrastructure optimization increases, IT labor, user labor, and downtime costs decrease, but hardware and software costs change little. As a result, as infrastructure optimization improves, hardware and software represent a larger part of TCO.

Cost Category	Category includes costs for…	Annual Cost per PC	Percentage Annual TCO
Direct Costs (IT Budget)			
Hardware and software	PC hardware, operating systems, and applications. Hardware and software costs are amortized over a period of 3 years.	$1,418	30%
IT Labor	IT labor used to manage desktops either through direct interaction with users and PCs or through management servers.	$630	15%
Indirect Cost (Unbudgeted costs incurred outside of IT)			
User Labor	Primarily user self-support and time spent learning to use IT systems. Microsoft research shows that a typical user spends between 60 and 120 hours per year in self-support activities.	$2,357	50%
Downtime	Lost user productivity caused by an IT system failure. Because users can often remain productive without their PC, this metrics is discounted by 80 percent.	$95	5%

Exhibit 5: Description and relative importance of TCO cost categories

This paper is organized into two major sections, which include:

- **"Understanding IT Labor Costs,"** which discusses how organizations spend their IT budget and how IT cost spending changes in organizations at different levels of infrastructure optimization.
- **"Implementing Best Practices with Management Software Technology,"** which summarizes how organizations can establish best practices by choosing and deploying current desktop and server management software.

Understanding IT Labor Costs

Although an organization's size and industry influenced IT labor costs, among organizations participating in this study, infrastructure optimization level was the dominant factor. This section provides infrastructure optimization and best practice adoption trends and discusses how costs change in organizations of different infrastructure optimization levels.

Infrastructure Optimization Trends

Participating organizations demonstrated infrastructure optimization in all but the most advanced level. Exhibit 6 shows how the 14 private enterprise organizations profiled in this study were distributed within the IOM.

IOM Level	Number of Organizations	Average PCs per Organization
Basic	4 (29%)	4,750
Standardized	8 (57%)	2,981
Rationalized	2 (14%)	7,550
Dynamic	0	0

Exhibit 6: Organization grouped by IOM categories

In Microsoft's IOM, 29 percent of the 14 enterprise organizations operate at the Basic level, and 57 percent operate at the Standardized level. Only 14 percent of the organizations achieved the Rationalized level, which enables them to run managed desktops and use advanced software features. No company showed an optimization status that qualified them for the Dynamic category.

Best Practices and Infrastructure Optimization

The number of best practices adopted by participating organizations was used as an indicator of their infrastructure optimization level—the more best practices adopted, the higher the infrastructure optimization level. Exhibit 7 shows the frequency distribution of organizations at each IOM level.

IOM Level	Average Number of Best Practices	Number of Organizations
Basic	0 to 2	4 (29%)
Standardized	3 or 4	8 (57%)
Rationalized	5 or 6	2 (14%)

Exhibit 7: Best practice adoption rates by IOM level

Of the 14 private enterprises participating in this study:

- Twenty-nine percent operated at the Basic level as indicated by adoption of two or fewer best practices. The most common best practice among organizations at the Basic level was adopting a single operating system. None of these organizations used a centrally managed firewall or automated software distribution.
- Fifty-seven percent of the sample operated at the Standardized level, as indicated by their adoption of any three or four of the six best practices. Standardized organizations clustered into two distinct groups with a roughly 20-percent difference in average IT labor costs. As in Basic organizations, firms in the higher-cost group of Standardized companies lacked a centrally managed PC firewall and automated software distribution. Organizations in the lower-cost group used these best practices and approached the average IT labor costs of Rationalized organizations.

- The remaining fourteen percent of the sample operated at the Rationalized level, as indicated by their adoption of five or six of the best practices, including desktop lockdown. Desktop lockdown is a combination of three best practices: users install only software sanctioned by their IT group, users can change only the PC settings that do not jeopardize reliability or security, and automated software distribution based on group membership.

Rather than just considering averages throughout this paper, it is useful to look at the top five performers (lowest-cost IT operations) to see how their costs relate to best practice adoption rates. Exhibit 8 presents the IT costs and best practice adoption rate of these lowest-cost operations.

Industry	IT Costs per PC	Average Number of Best Practices
Hospitality	$260	6
Financial services	$263	6
Oil and gas	$322	4
Healthcare	$379	3
Transportation	$405	3

Exhibit 8: IT costs of lowest-cost IT operations

As expected, organizations that adopted six best practices have the lowest IT labor costs, which gradually increase as the number of best practices decreases. All five of these organizations also had a comprehensive security program with centrally managed PC firewalls and automated software distribution for patching and PC application deployment.

The Industry Effect

Although this paper focuses on 14 private enterprises to emphasize the connection between infrastructure optimization and IT labor costs, the initial research also included 17 government and educational organizations. If analyzed separately, each of these groups show the same behavior—the more best practices in use, the lower the IT labor costs. However, when the three groups are evaluated as a single sample, the effect of infrastructure optimization on IT costs is less clear. This industry effect occurs because each of the three groups has its own cost and best practice profile.

For example, educational organizations, which have the lowest cost profile, also have the lowest best practice adoption rate. On the other end of the spectrum, government organizations have both the highest costs and the highest best practice adoption rate. When data from educational, private enterprise, and government organizations are combined, the relationship between best practice adoption rates and IT labor costs is diluted because of the industry variables.

Exhibit 9 shows the average annual IT labor costs and average number of best practices adopted by each group.

Organization Type	IT Costs per PC	Number of Organizations	Average Number of Best Practices
Educational	$334	8	2.8
Private enterprise	$568	14	3.0
Government	$624	9	3.3

Exhibit 9: Effect of organization industry on IT costs and best practice adoption

Exhibit 10 presents IT cost and best practice data twice, once for 14 private enterprises and again for the 31-organization sample. Although best practice adoption rates remain relatively constant in each sample, the differences in IT costs between Basic and Rationalized infrastructure optimization levels is greater in the private enterprise sample.

	Private Enterprises			All Organizations		
IOM Level	IT Labor Costs per PC	Average Number of Best Practices	Number of Organizations	IT Labor Costs per PC	Average Number of Best Practices	Number of Organizations
Basic	$774	1.4	4	$618	1.4	13
Standardized	$542	3.6	8	$488	3.6	12
Rationalized	$261	6.0	2	$391	5.7	6

Exhibit 10: Annual IT labor costs for enterprise organizations and entire sample

Effects of Organizational Size

Of the three variables analyzed in this study, organization size has the weakest influence on IT labor costs. Study results show that there is no significant connection between infrastructure optimization level and the number of PCs in an organization. Exhibit 11 provides the average annual IT labor costs per PC for three size classes of organization.

PCs per Organization	IT Labor Costs per PC	Number of Organizations	Average Number of Best Practices
1,500 - 3,000	$551	12	3.3
3,001 - 5,000	$499	10	2.9
5,001 - 13,500	$425	9	3.0

Exhibit 11: IT labor costs per PC by organization size

As a general rule, IT costs decline at a modest rate of about $10 per PC for each 1,000 PCs deployed. This relationship is valid between 1,000 and 10,000 PCs.

IT Labor Costs at Different Levels of Infrastructure Optimization

In this study, IT effort that supports PCs was grouped into three categories: direct PC support, service desk, and PC management with servers.

Direct PC support costs. This category includes costs for image engineering, security management, PC deployment, portfolio management, and application packaging and testing. This cost category is highly sensitive to the number of operating systems in use and the ability of an IT department to deliver applications and patches with automated software distribution.

Service desk costs. These are the staffing costs needed to operate the help desk and engage the personnel, who repair failed PCs that cannot be repaired remotely. This cost category is primarily affected by the PC firewalls, limiting users to installing only IT-sanctioned software, preventing changes to PC settings that jeopardize PC reliability or security, and automating password resets.

Server-based management costs. This category includes the labor costs of personnel, who engage in systems management, directory administration, and setting PC policy. These are the people who manage tools such as SMS, manage directory infrastructures such as Active Directory, and create, test, and implement PC policies such as Microsoft Windows Group Policies. IT costs in this category are very sensitive to the degree of infrastructure standardization.

IT Labor Costs and Infrastructure Optimization

As organizations move from one optimization level to another, IT cost savings and the effects of management technologies that make these savings possible also change. This section describes the effects of management tools used by organizations in this study on system complexity and IT labor costs. Exhibit 12 provides an overview of average annual IT labor costs for organizations at each IOM level.

IOM Level	Total IT Labor Costs per PC
Basic	$774
Standardized	$542
Rationalized	$261

Exhibit 12: Average IT labor costs at each IOM level

By moving from the Basic to the Standardized level, organizations in this study saved $232 per PC per year, a 30-percent savings. Moving from the Standardized to Rationalized optimization saved organizations even more, $281 per PC per year, or a 52-percent savings.

As organizations progress to new optimization levels, cost savings are also affected by organizations' systems management infrastructures, which consist of systems management tools, directories, and PC policies. At the Basic level, organizations had almost no systems management infrastructure. At the Standardized level, organizations used a mixture of overlapping tools. Complexity at the Standardized level decreased management efficiency and increased costs. At the Rationalized level, organizations standardized on one set of tools that were used throughout the company. Exhibit 13 shows the average number of management tools used by organizations at each IOM level.

IOM Level	Average Number of Management Products Supported
Basic	0.3
Standardized	2.0
Rationalized	1.5

Exhibit 13: Management products supported at each IOM level

Moving from Basic to Standardized Optimization

Organizations at the Basic optimization level managed their PC environments with few if any management tools, an average of 0.3 systems management products per organization. A lack of tools prevented these organizations from automating software distribution and implementing a comprehensive security program with a centrally managed firewall. Use of these two best practices was the largest differentiator between organizations with high and low IT labor costs.

Moving from Standardized to Rationalized Optimization

Organizations at the Standardized level used more management tools than organizations at other optimization levels. However, these organizations often used as many as four different systems management products from different vendors to manage different portions of their PC environment. This approach added system complexity, reduced the ability to implement best practices uniformly across their organizations, and drove up server management costs. Study results show that to reach Rationalized optimization, Standardized organizations must:

- Reduce complexity by standardizing on a single PC operating system, one directory, and the minimum number of systems management tools required to deliver required functionality.
- Implement a centrally managed firewall and automated software distribution (if this has not been done previously). These capabilities enable organizations to join the Standardized level's lower-cost IT operations group cited previously.
- Limit users' ability to install software and change PC settings by locking down the desktop.

Rationalized organizations in this study had enough tools to adopt all six best practices but minimized the number of tools to reduce system complexity. This approach reduced IT costs and made it easier to implement five or six best practices across their organizations.

Implementing Best Practices with Management Software Technology

Previous sections have shown how optimizing IT infrastructures and adopting best practices can reduce IT labor costs. This section describes the six best practices, how they affect costs, and the technologies needed to implement them.

Best Practices, IT Process Efficiency, and IT Costs

Adoption of best practices is a strong predictor of IT cost savings. Research for this paper collected data on 21 best practices, which ranged from application compatibility testing to user provisioning. Of the 21 best practices studied, only six showed a strong relationship with reduced IT labor costs. Research results showed that although the remaining 15 best practices provided value, there were no consistent trends that held true for all 31 organizations participating in this study. Although some organizations achieved significant cost savings by using these best practices, others achieved few savings or none at all.

Exhibit 14 shows the relationships between adopting a specific best practice, the resulting IT cost savings, and the enabling Microsoft technology that makes these savings possible.

Best Practice	IT Cost Savings per PC	Number of Organizations	IT Administrative Tasks	Microsoft Enabling Technology
Standardize on a single PC operating system	$52	9	▪ Image management ▪ Desktop administration ▪ Service desk and desk-side support	▪ Windows 2000 or newer operating system
Users can install only IT-sanctioned software	$50	7	▪ Application management ▪ Desktop administration ▪ Service desk and desk-side support	▪ Active Directory and Group Policies ▪ Microsoft Installer ▪ Systems Management Server ▪ Windows 2000 or newer operating system
Centrally managed PC firewall	$39	7	▪ Security and patching ▪ Desktop administration ▪ Service desk and desk-side support	▪ Active Directory and Group Policies ▪ Windows XP SP2 or newer operating system
Users can only change PC settings that do not compromise reliability or security	$30	9	▪ Application management ▪ Desktop administration ▪ Service desk and desk-side support	▪ Active Directory and Group Policies ▪ Windows 2000 or newer operating system
Automated password reset	$29	7	▪ Service desk and desk-side support	▪ Microsoft technology not yet available
Automate software distribution based on group membership	$26	8	▪ Application management ▪ Desktop administration ▪ Security and patching	▪ Active Directory and Group Policies ▪ Microsoft Installer ▪ Systems Management Server

Exhibit 14: IT cost savings, best practices, and their enabling software technologies

The PC firewall and automated software distribution best practices do not provide organizations with the largest cost savings. Nevertheless, of the six best practices used in this study, these best practices were the strongest predictor of IT

labor costs. If the 14 organizations in this study are ranked from low (starting at the top) to high cost, the bottom six organizations have neither the centrally administered firewall nor automated software distribution.

Standardize on a Single Desktop Operating System

Organizations that standardized on a single desktop operating system saved IT costs compared to organizations that ran more than one operating system. Organizations that ran a single operating system significantly reduced the complexity of their PC environment and their IT labor costs. Those that did not adopt this practice duplicated substantial effort in application compatibility testing and image management.

To implement this best practice, organizations need to automate PC operating system upgrades to make the process more cost-effective. Many organizations that run more than one operating system do so out of necessity instead of choice. Because of a lack of infrastructure optimization, they are forced to rely on the PC hardware refresh cycle to deploy their PCs. As a result, they use the operating system that is shipped with the PC. Because PCs are replaced over time, but different operating systems are sold, organizations end up with a mix of operating systems in their IT environments.

This best practice delivers cost savings to organizations running one desktop operating system rather than two. Organizations that run more than two operating systems can expect greater cost savings than those assigned to this best practice. One of the organizations featured in this research ran four PC operating systems; after standardizing, its IT labor costs decreased to the lower 25 percent of the sample.

Users Can Install Only IT-Sanctioned Software

There is a direct correlation between the complexity of an organization's application portfolio and IT labor costs. When IT groups decide which applications are installed on users' PCs, they simplify portfolio management and prevent undocumented and poorly written applications from generating support calls, compromising security, and interfering with future system upgrades.

Many organizations can control the installation of unauthorized software. However, by adopting this best practice, organizations might reduce end-user satisfaction with the IT department and reduce end-user agility. Before making a decision to claim $50 of the total $226 best practice IT cost benefit, organizations should balance the cost savings against the quality of the end-user experience. Many organizations will choose to absorb the cost rather than reduce the effectiveness of their PC users.

Ensuring that users install only IT-sanctioned software requires a centrally managed directory and group policies to configure PC settings and an automated method for deploying applications. Users must also be given Standard User rights instead of Administrative rights to prevent them from overriding IT policies.

Centrally Managed PC Firewall

Although this study tracked PC firewall usage, this best practice is better defined as a comprehensive security program. Most of the organizations that used a centrally managed PC firewall did so as part of a larger security program, which included network access control and other programs designed to reduce exposure to security risks.

This best practice reduces costs in two ways. First, PC firewalls reduce security breaches from hackers and prevent some virus attacks. This benefit reduces service desk calls and the amount of time IT personnel spend repairing security breaches. Second, managing a PC firewall from a centralized location enables IT organizations to defend against attacks proactively and reduces reactive patching. For example, when a new virus that attacks a specific port is discovered, the IT staff can close that port on every PC throughout the organization, rendering the virus inert. Then, the IT staff has time to locate a security update, test it, and add it to the normal system maintenance cycle. After the security update is deployed, the port can be re-opened.

If this capability is unavailable when an organization experiences a virus attack, some or all of the PCs in the IT infrastructure would be affected and require an expensive cleanup. Even if organizations do not experience an attack, the IT staff would have to launch an emergency effort to update all PCs to remove the security vulnerability. This approach is substantially more expensive and risky than delivering a security update through a normal maintenance cycle.

Users Can Change Only IT-Sanctioned PC Settings

This best practice helps IT groups avoid jeopardizing PC reliability and security. It is often implemented with the best practice that permits users to install only IT-sanctioned software.

This best practice provides two benefits. First, users are prevented from harming their PC by editing the system registry or changing security settings. For example, even if an organization implements a centrally managed firewall, without IT control over PC settings, users can open ports at will, making their PC vulnerable. In this situation, users may choose to open ports to accommodate applications such as Web phones or chat sessions. Second, with more settings set by the IT group, PCs are more standardized, which reduces troubleshooting costs.

Adopting this best practice is less controversial than the practice that controls installed software applications because fewer users directly edit registry and security settings. However, the infrastructure requirements for both of these best practices are similar: users must be assigned only Standard User access, and policies must be implemented through a directory.

Automated Password Account Reset

This best practice prevents many calls to the service desk that occur when users forget their passwords or their passwords expire when they are on vacation or sick leave.

The value of this best practice is often linked to an organization's infrastructure optimization level. Basic and Standardized organizations are typically very complex and operate non-integrated systems. Users at these organizations must remember a large number of passwords, which can make password-related problems worse. High levels of system complexity also prevent Basic and Standardized organizations from providing automatic password reset capabilities on all their systems. At these organizations, there are too many line of business applications to automate password processes. Rationalized organizations on the other hand, have engineered complexity out of their environment and are more likely to use a metadirectory that synchronizes passwords and user identities across systems. In these advanced IT environments, passwords are reset in the metadirectory and are propagated to all systems.

Implementing this best practice requires a software program for resetting passwords for each line of business application with user identities and passwords.

Automated Software Distribution

Automated software distribution enables the IT staff to install software updates and applications without the direct intervention of IT personnel or users. This approach enables the IT staff to deliver software to any number of PCs simultaneously and reduces the time required to close a security vulnerability with an update.

In small organizations, software can be distributed with a directory-based system that pushes software and delivers security updates to PCs with policies or that publishes optional software for users to install on demand. Larger organizations generally require more sophisticated systems management software that can balance loads during large rollouts and consider more parameters before pushing the software to users.

Complete Desktop Lockdown

Complete desktop lockdown is a combination of three best practices: users can install only IT-sanctioned software, users can change only IT-sanctioned PC settings, and automated software distribution. As a group, these three best practices represent $106 per PC per year or 47 percent of the total $226 annual value of best practice-related benefits. Implementing this best practice involves all of the prerequisites of the individual practices described previously.

Value of Operating Directory Services

Of the management-related software, directory services had the greatest influence on IT labor costs. Directories are also the single Microsoft technology that had a role to play in all six best practices presented in this paper.

Using the Active Directory service and Group Policies reduced annual IT labor costs by $183 per PC ($171 if organizations that used SMS are not included). Of the 14 private enterprise organizations in the sample, nine used Active Directory, while the other five used a flat directory service such as Windows NT® Server version 4.0 domains or Novell Netware 3.x. (Novell e-Directory was not represented in the sample.)

Exhibit 15 shows the relationship between the directory service used, IT labor costs, and best practice adoption rate.

Directory Service	IT Labor Costs per PC	Average Number of Best Practices	Number of Organizations
Active Directory	$503	3.9	9
Flat directory[4]	$686	2.2	5

Exhibit 15: Operating system directory usage trends

All six best practices profiled are directly related to the use of Active Directory.

- **Standardize on a single operating system.** Active Directory can transfer user information during a PC upgrade, making it easier to standardize on a single operating system.
- **Users can install only IT-sanctioned software.** Active Directory with Group Policies enables IT professionals to assign installation permissions appropriate to each user.
- **Centrally managed PC firewall.** Active Directory and Group Policies are used to configure PC firewalls and can alter configurations in response to a security threat.
- **Users can change only IT-sanctioned PC settings.** Active Directory and Group Policies enable IT professionals to assign PC configuration permissions appropriate to each user.
- **Automated password reset.** Active Directory can be used with Microsoft Identity Integration Server (MIIS)[5] to reset passwords in Active Directory and other directory and identity repositories. If a password is reset in Active Directory, MIIS propagates the changes to other systems, to which users need access. Although MIIS reduces the complexity of identity management, third-party software must be used to provide additional functionality to enable users to reset passwords without service desk assistance.
- **Automated software distribution.** For small organizations, Active Directory and Group Policies can push software to PCs with Windows Installer files or advertise an application for a user to pull down. Larger organizations will use SMS for automated software deployment.

Value of Management Software

Management software had the second largest impact on IT labor costs. Active Directory and SMS were tightly linked in this study; all organizations running SMS also ran Active Directory. Separating the benefits of the two products was difficult, and some of the benefits attributed to Active Directory might belong to SMS. Organizations that ran SMS with Active Directory saved $28 per PC per year more than those that ran Active Directory alone and saved $93 per PC per year more than organizations that used no management software.

Exhibit 16 provides the average annual IT labor cost per PC and best practice adoption rates for SMS, competitive management software, and no management software.

Management Software	IT Labor Costs per PC	Average Number of Best Practices Adopted	Number of Organizations
SMS	$487	4.0	4
Non-Microsoft software[6]	$649	4.0	3
None	$580	2.5	7

Exhibit 16: Annual IT costs and best practice adoption rates by types of management software

Results in Exhibit 16 imply that organizations that use non-Microsoft systems management tools spend more than firms that run no systems management tools. This is not necessarily true. There were other mitigating factors. All

[4] Windows NT 4.0 or Novell Netware 3.x.

[5] For more information on Microsoft Identity Integration Server go to http://www.microsoft.com/windowsserversystem/miis2003/default.mspx.

[6] Novell ZenWorks, LANDesk, Altiris (usually with SMS), IBM Tivoli, and Computer Associates Unicenter

of the organizations in this category ran more than one desktop operating system; one organization operated four. This had a very negative effect on these organizations' costs. The willingness to run multiple desktop operating systems carried over to the management software itself. Most of these organizations ran different management products in different parts of their organization. As a result, there was significant duplication of effort and no economies of scale. The high cost of the non-Microsoft tools had more to do with complexity than a lack of capability of the products.

Use of SMS was linked to three of the six best practices described in this study:

- **Standardize on a single operating system.** SMS can significantly reduce the cost of operating system upgrades by automating user migrations and reducing imaging costs.
- **Users install only IT-sanctioned software.** When users cannot install software, the IT department can use SMS automated software distribution to install it for them.
- **Automated software distribution.** Automated software distribution is a key component of SMS capabilities.

Value of PC Operating Systems

The choice of PC operating system had less effect on IT labor costs than the choice of directories and management software. In general, organizations that run more than one PC operating system increase system complexity and experience a large increase in IT labor costs. Exhibit 17 compares the annual IT labor costs of organizations that run Windows XP, Windows 2000, or both.

Desktop Operating System	IT Labor Costs per PC	Average Number of Best Practices	Number of Organizations
Windows XP	$516	3.4	7
Windows 2000	$534	3.5	2
Windows XP and Windows 2000	$655	3.2	5

Exhibit 17: Operating systems and IT labor costs

Windows 2000, Windows XP, and Windows XP Service Pack 2 are compatible with Group Policies. These desktop operating systems enable IT departments to assign application installation and PC configuration permissions to users. Windows XP Service Pack 2 provided additional functionality through its built-in firewall and IT management capabilities of Active Directory and Group Policies. Windows 2000 and Windows XP required third-party products to reach the same level of functionality. These additional software products increased complexity and IT labor costs.

Value of Microsoft Windows Vista

Although the research of this study pre-dates the release of the Microsoft Windows Vista client operating system, it is possible to predict the potential effect that using Windows Vista will have on infrastructure optimization and best practice adoption. Features in Windows Vista will make it easier to implement four of the six best practices profiled in this study. Exhibit 18 describes the Windows Vista features that can be used to implement these best practices.

Best Practice	Selected Windows Vista Features
Standardize on a single operating system.	▪ Registry and directory virtualization
Users can install only IT-sanctioned software.	▪ User Account Control (UAC) ▪ Registry and directory virtualization
Centrally managed PC firewall	▪ Windows Vista firewall
Users can change only IT-sanctioned PC settings.	▪ User Account Control ▪ Registry and directory virtualization

Exhibit 18: Windows Vista features that support best practices

Windows Vista capabilities are related to four of the study's six best practices:

- **Standardize on a single operating system.** Windows Vista registry and directory virtualization will reduce the number of application compatibility problems. Application compatibility was a barrier for some organizations, which needed to keep older operating systems to accommodate legacy applications that were too expensive to replace.
- **Users can install only IT-sanctioned software.** One of the barriers to implementing this best practice was the requirement of giving users administrative rights to their PCs to accommodate legacy applications, which would only run under users in this context. The combination of UAC and virtualization will make it possible to redirect many of these applications into running in the Standard User context. These features make it possible for organizations that have a centralized directory that can deliver PC policies and a systems management infrastructure to implement this best practice without replacing a large number of applications or buying third-party party workarounds.
- **Centrally managed PC firewall.** The improved firewall capability in Windows Vista and related group policies enable greater centralized control of ports and packet filtering than was possible with Windows XP Service Pack 2.
- **Users can change only IT-sanctioned PC settings.** One of the barriers to IT groups controlling PC configurations was the requirement of giving users administrative rights to their PCs to accommodate legacy applications, which would only run under users in this context. The combination of UAC and virtualization makes it possible to redirect many of these applications into running in Standard User context. These features make it possible for organizations with the proper directory and systems management infrastructure to implement this best practice without replacing a large number of applications or buying third-party party workarounds.

Conclusions and Recommendations

Adopting best practices reduces IT labor costs, but system complexity increases them. This theme is repeated throughout this paper. Adopting best practices that optimize IT infrastructures and choosing directory and management server software that decreases system complexity can help virtually any organization reduce IT labor costs.

This study summarizes results of research conducted in 2005 at 14 private enterprise organizations. Study results show that organizations can improve their infrastructure optimization level and reduce annual IT labor costs by:

- Saving up to $226 per PC in IT labor costs by adopting the six best practices described in this study.
- Using Windows Active Directory, Group Policies, and Systems Management Server to increase best practice adoption rates and save organizations up to $199 per PC per year.

Organizations can significantly reduce IT labor costs by reducing infrastructure complexity when they:

- **Standardize on a single operating system.** Organizations that deploy only one PC desktop operating system pay $52 per PC less in annual IT labor costs than organizations that do not standardize.
- **Standardize on management software.** Standardizing on one management product can significantly reduce management costs and make it easier for organizations to implement best practices.

Organizations improve their infrastructure optimization level by engineering complexity out of their environments—by standardizing on one PC operating system, directory, and systems management product. After the complexity is reduced, best practices become easier to adopt, making it easier to achieve the annual $226 per PC benefit. These savings will likely pay for the cost of the upgrades.

Recommendations

Optimizing IT infrastructures requires different strategies that depend on an organization's current infrastructure optimization level and supporting IT infrastructure. Organizations considering infrastructure optimization should focus on improving infrastructure optimization one level at a time and then stabilizing their IT systems and processes instead of skipping a level.

Basic organizations. Basic organizations need to focus on:

- Developing and implementing a five-year PC strategy that is based on hardware refresh cycles and spans at least two deployments.
- Implementing Active Directory and Group Policies to accomplish basic PC management tasks.
- Deploying Microsoft Windows Vista after a PC strategy and desktop management capabilities are established.

With a PC refresh cycle in place, several different Windows Vista deployment options become possible. Organizations should perform financial modeling on manual deployments and managed diversity (a hardware refresh cycle) as a means of deploying Windows Vista.

Because organizations are in different situations, there is no "one size fits all" solution. However, adopting best practices and simplifying IT infrastructures to reduce IT labor costs was a common theme that occurred often throughout this study. By implementing Active Directory and Group Policies, organizations can centralize the management of Windows Vista capabilities and maximize the value of the operating system deployment.

Standardized organizations. Standardized organizations should:

- **Use Group Policies aggressively** to enforce IT standards and lock down PC desktops. This approach might require consolidation of the directory infrastructure to reduce complexity.
- **Deploy systems management software** to deploy applications and security updates. Automated software distribution is a prerequisite to full lockdown because in this configuration, users install only IT-sanctioned software applications.

- **Standardize on one management suite** rather than increasing system complexity—and costs—by using more than one product.
- **Make the deployment of Windows Vista a priority** because new features such as UAC and directory and file system virtualization will make it possible for IT organizations to control which settings are changed on PCs and which software can be installed. Active Directory and Group Policies also manage other Vista features, such as an improved firewall, power saving modes, and spyware and malware settings for Microsoft Internet Explorer. These features will add value to optimized IT infrastructures.

Moving from Standardized to Rationalized levels of infrastructure optimization requires limiting users' ability to change PC settings and preventing the installation of non-IT sanctioned software. This change can be accomplished with the use of Active Directory, Group Policies, and Systems Management Server. Windows Vista will make it much easier to reach this goal with new technologies that put users in Standard User context. Without using Vista, many organizations would have to replace a significant number of applications or purchase third-party utilities, which would increase system management complexity. Because complexity drives up IT labor costs, in virtually all cases, Vista will be the least expensive way to standardize on a single operating system, manage PC settings, and control which software is installed on user PCs.

Rationalized organizations. Rationalized organizations, which already use the six best practices described in this paper, should focus on other priorities. Instead of concentrating solely on IT costs, these organizations will be driven by business value measured by improved business agility, increased user productivity, and reduced risk exposure.

To improve agility, these organizations should look for additional ways to simplify their IT infrastructures. The simpler an IT environment, the easier it is to reconfigure it to adapt to new business requirements. Windows Vista will add value as a development platform, because new technologies such as improved managed code based on the Microsoft .NET® Framework will reduce the time it takes to create, deploy, and manage new applications.

Although new capabilities in Windows Vista will have positive cost benefits, reduced time to market will be the driver at organizations that are trying to change their infrastructure optimization level from Rationalized to Dynamic. Increasing user productivity will be part of an information worker strategy. Windows Vista can play a role in this IT strategy by making it easier for users to set up small workgroups and share information.

Many Rationalized organizations will choose to roll out Windows Vista with the 2007 version of the Microsoft Office System. Reducing security risk will require new best practices and technologies that might increase IT costs. A good example of this phenomenon is Smartcards, which protect user identity and information but require IT resources to implement and maintain. Windows Vista, with its more secure code base, firewall, and hardened Microsoft Internet Explorer, can also contribute to lower risk.

Appendix A: About This Study

In August 2005, Microsoft engaged GCR Custom Research, a custom market research firm located in Portland, Oregon, to interview 150 organizations in the United States about their IT staffing, technology, and processes. This project was one of a dozen studies designed to identify the largest cost categories in the Microsoft Windows environment and to use this information to improve future Microsoft products.

Of the original 150 datasets generated by this research, 31 were used in this paper. The remaining 119 were disqualified because:

- Respondents were responsible for fewer than 1,000 or more than 15,000 PCs.
- Respondents were unable to answer all of the questions asked in the interview.
- Internal data checks revealed inconsistencies in the data that respondents provided.

Participants were chosen by GCR Custom Research without any involvement from Microsoft. The only criteria used were that respondents should operate in the United States and have more than 1,500 PCs in their organizations. In most cases, respondents were chief information officers, corporate vice presidents, or director-level managers.

Most of the data came from retail, financial services, healthcare, government, and educational organizations. The average interview lasted 90 minutes and focused on IT staffing, technologies, and processes. Respondents were not paid for their time.

The survey was developed by GCR Custom Research and Microsoft. GCR Custom Research provided Microsoft with the raw data; Microsoft performed all analyses. All views expressed in this paper are those of Microsoft Corporation.

About the Author

William Barna is a senior program manager in the Windows Enterprise Management Division in Microsoft's headquarters at Redmond, Washington. In this role, he conducts TCO research and provides this information to product teams to improve future Microsoft products. Before working in Redmond, he worked as a Senior Consultant for Microsoft Consulting Services (MCS) in Dallas, Texas. He focused on business value consulting and worked extensively with the Rapid Economic Justification (REJ), TCO, and Rapid Portfolio Alignment (RPA) programs. He also performed technical engagements working with Active Directory, Group Policies and Systems Management Server.

Before coming to Microsoft, Barna worked for KPMG Peat Marwick as a senior consultant and project manager in the United States and Europe. He has a BS degree in Political Science from the University of California at Davis and an MBA degree from Southern Methodist University in Dallas. Barna has completed graduate work in international business and computer science at ESC Rouen in France, WHU Koblenz in Germany, and the University of Maryland.

Appendix B: Infrastructure Optimization

The Infrastructure Optimization Model from Microsoft helps customers understand and subsequently improve the current state of their IT infrastructure and what that means in terms of cost, security risk and operational agility. Dramatic cost savings can be realized by moving from an unmanaged environment towards a dynamic environment. Security improves from highly vulnerable in a Basic infrastructure, to dynamically proactive in a more mature infrastructure. IT Infrastructure Management changes from highly manual and reactive to highly automated and proactive. Microsoft and Partners can provide the technologies, processes and procedures to help customers move up through the Infrastructure Optimization Journey. Process moves from fragmented or non-existent to optimized and repeatable. A customer's ability to use technology to improve their business agility and deliver business value increases as they move from the Basic state up the continuum toward a Dynamic state empowering information workers, managers and supporting new business opportunities.

By working with Microsoft and using this model as a framework, an enterprise can quickly understand the strategic value and business benefits to the organization in moving from a "basic" level of maturity (where the IT infrastructure is generally considered a "cost center") towards a more "dynamic" use when the business value of the IT infrastructure is clearly understood and the IT infrastructure is viewed as a strategic business asset and business enabler.

Infrastructure Optimization Model in Action

The Microsoft Infrastructure Optimization Model was developed by using industry best practices and Microsoft's experience with enterprise customers. A key goal for Microsoft in creating the Infrastructure Optimization Model was to develop a simple way to use a maturity framework that is flexible and can be used easily as the benchmark for technical capability and business value.

The first step in using the model is to evaluate what maturity level you are at in the model. Once the current maturity level has been established, the next step is to use the model to develop a plan on how to progress through each maturity level in order to reach the target level needed for maximum business benefit.

Level 1: Basic

The Basic IT infrastructure is characterized by manual, localized processes, minimal central control, non-existent or un-enforced IT policies and standards regarding security, backup, image management and deployment, compliance, and other common IT standards. There is a general lack of knowledge regarding the details of the infrastructure that is currently in place or which tactics will have the greatest impact to improve upon it. Overall health of applications and services is unknown due to a lack of tools and resources. There is no vehicle for sharing accumulated knowledge across IT. Customers with Basic infrastructure find their environments extremely hard to control, have very high desktop and server management costs, are generally very reactive to security threats and have very little positive impact on the ability of the business to benefit from IT. Generally all patches, software deployments, and services are provided high touch and high cost.

Customers benefit substantially by moving from this type of Basic Infrastructure to a Standardized Infrastructure helping them to dramatically reduce costs through:

- Developing standards, policies, and controls with an enforcement strategy
- Mitigating security risks by developing a "defense in depth" posture – a layered approach to security at the perimeter, server, desktop and application levels
- Automating many manual and time consuming tasks
- Adopting "best practices" (ITIL, SANS, etc.)
- Aspiring to make IT a strategic asset rather than a burden

Level 2: Standardized

The Standardized infrastructure introduces controls through the use of standards and policies to manage desktops and servers, how machines are introduced to the network, the use of Active Directory to manage resources, security policies, and access control. Customers in a Standardized state have realized the value of basic standards and some policies yet are still quite reactive. Generally all patches, software deployments and desktop service are provided through medium touch with medium to high cost. However, they have a reasonable inventory of hardware and software and are beginning to manage licenses. Security measures are improved with a locked down perimeter, internal security may still be a risk.

Customers benefit by moving from this Standardized state to a Rationalized state with their infrastructure by gaining substantial control over the infrastructure and having proactive policies and processes that prepare them for the spectrum of circumstances from opportunity to catastrophe. Service Management is a concept and the organization is taking steps to recognize where to implement it. Technology is also beginning to play a much larger role moving toward a Rationalized infrastructure by becoming a business asset and ally rather than a burden.

Level 3: Rationalized

The Rationalized infrastructure is where the costs involved in managing desktops and servers are at their lowest and processes and policies have matured to begin playing a large role in supporting and expanding the business. Security is very pro-active and responding to threats and challenges is rapid and controlled.

The use of Zero Touch Deployment minimizes cost, time to deploy and technical challenges. The number of images is minimal and the process for managing desktops is very low touch. They have a clear inventory of hardware and software, and only purchase those licenses and computers they need.

Security is extremely pro-active with strict policies and control from desktop to server to firewall to extranet.

Customers benefit on a business level by moving from this Rationalized state to a Dynamic state. The benefits of implementing new or alternative technologies to take on a business challenge or opportunity far outweigh the incremental cost. Service Management is implemented for a few services with the organization taking steps to implement more broadly across IT. Customers contemplating the value of Dynamic state generally are looking for their IT infrastructure to provide business advantage.

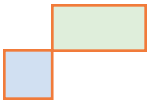
Level 4: Dynamic

Customers with a Dynamic infrastructure are fully aware of the strategic value their infrastructure provides in helping them run their business efficiently and staying ahead of competitors. Costs are fully controlled, integration between users and data, desktops and servers, collaboration between users and departments is pervasive and mobile users have nearly on-site levels of service and capabilities regardless of location.

Processes are fully automated, often incorporated into the technology itself allowing IT to be aligned and managed according to the business needs. Additional investments in technology yield specific, rapid, measurable benefits for the business.

The use of self provisioning software and quarantine-like systems for ensuring patch management and compliance with established security policies allows the dynamic organization to automate processes, thus improving reliability, lowering costs and increasing service levels.

Customers benefit from increasing the percentage of their infrastructure that is Dynamic by providing heightened levels of service, competitive and comparative advantage and taking on bigger business challenges. Service Management is implemented for all critical services with service level agreements and operational reviews established.



www.microsoft.com

Microsoft