

Core Infrastructure Optimization   
Implementer Resource Guide:   
Standardized to Rationalized

Published: April 2007

Abstract

The vision of infrastructure optimization is to build an efficient, secure, and optimized information technology (IT) infrastructure and services in a logical sequence. An optimized IT infrastructure is built upon IT standards and ensures conformation to those standards. Improvements to the IT infrastructure at each level of optimization can bring about significant cost reduction, increased security, and improved availability and manageability.

This is the second of three resource guides explaining key IT capabilities necessary to move from one of four defined levels of IT services to the next more efficient and streamlined level of services. This document briefly describes each of the four levels and explains each capability in the Microsoft® Core Infrastructure Optimization Model. It then introduces high-level concepts for planning, building, deploying, and managing these capabilities and provides links to relevant resources where more detailed and actionable content can be found. You can use the information contained in this guide to help you move from the Standardized level to the Rationalized level.

For the latest information and for more detailed descriptions and business benefits of the Microsoft Infrastructure Optimization Model, go to <http://www.microsoft.com/technet/infrastructure>.

Copyright © 2007 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation.  Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Active Directory, Active Sync, ActiveX, BitLocker, DirectX, Excel, Internet Explorer, Outlook, SharePoint, Windows, Windows Mobile, Windows NT, Windows Server, Windows Server System, and Windows Vista 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.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose.  You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback.  You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized 1](#_Toc164524266)

[Resource Guide Overview 1](#_Toc164524267)

[Audience 1](#_Toc164524268)

[Infrastructure Optimization Concept 1](#_Toc164524269)

[Core Infrastructure Optimization Capabilities 3](#_Toc164524270)

[Core Infrastructure Optimization Model Levels 3](#_Toc164524271)

[Core Infrastructure Optimization Capability Overview 5](#_Toc164524272)

[Capability: Identity and Access Management 19](#_Toc164524273)

[Introduction 19](#_Toc164524274)

[Requirement: Centralized Directory-based Configuration and Security 20](#_Toc164524275)

[Capability: Desktop, Device and Server Management 27](#_Toc164524276)

[Introduction 27](#_Toc164524277)

[Requirement: Automated Operating System Distribution 28](#_Toc164524278)

[Requirement: Automated Tracking of Hardware and Software for Desktops 33](#_Toc164524279)

[Requirement: Latest Two OS Versions and Service Packs on Desktops 39](#_Toc164524280)

[Requirement: Latest Versions of Microsoft Office on Desktops 46](#_Toc164524281)

[Requirement: Compatibility Testing and Certification of Software Distributions 53](#_Toc164524282)

[Requirement: Patch Management for Servers 58](#_Toc164524283)

[Requirement: Guaranteed Secure Communications with Mobile Devices 59](#_Toc164524284)

[Requirement: Access to Web Applications Using WAP or HTTP for Mobile Devices 62](#_Toc164524285)

[Requirement: Server Consolidation and Virtualization 65](#_Toc164524286)

[Requirement: Layered Imaging for Desktops 69](#_Toc164524287)

[Capability: Security and Networking 75](#_Toc164524288)

[Introduction 75](#_Toc164524289)

[Requirement: Policy-managed Firewalls on Servers and Desktops 76](#_Toc164524290)

[Requirement: Secure Remote Access to Internal Resources and LOB Applications 79](#_Toc164524291)

[Requirement: Secured and Guaranteed Communication Verification Between Servers 83](#_Toc164524292)

[Requirement: Service Level Agreement Monitoring and Reporting for Servers 88](#_Toc164524293)

[Requirement: Secure Communication Mechanism for Presence 93](#_Toc164524294)

[Requirement: Active Directory and IAS/RADIUS for Wireless Network Authentication and Authorization 98](#_Toc164524295)

[Requirement: Centrally Managed Certificate Services 104](#_Toc164524296)

[Requirement: Proactively Managed Bandwidth to Branch Offices 110](#_Toc164524297)

[Capability: Data Protection and Recovery 119](#_Toc164524298)

[Introduction 119](#_Toc164524299)

[Requirement: Centrally Managed Data Backup for Branch Offices 120](#_Toc164524300)

[Requirement: Backup, Restore, and Defined Recovery Times for Servers 124](#_Toc164524301)

[Capability: Security Process 127](#_Toc164524302)

[Introduction 127](#_Toc164524303)

[Requirement: Two-Factor User Authentication, Standard Security Review for New Software Acquisitions, and Data Classification Processes 128](#_Toc164524304)

[Capability: ITIL/COBIT-based Management Process 133](#_Toc164524305)

[Introduction 133](#_Toc164524306)

[Requirement: Operating, Optimizing, and Change Processes 133](#_Toc164524307)

[Additional Resources: Tools and Technologies 149](#_Toc164524308)

[Additional Resources: Standardized to Rationalized Checklist 153](#_Toc164524309)

Core Infrastructure Optimization   
Implementer Resource Guide:   
Standardized to Rationalized

This document provides a technology roadmap for implementing information technology (IT) capabilities highlighted in the Microsoft Infrastructure Optimization Model (explained in the following sections). We recommend that you use the steps outlined in this guide to become familiar with the tools, processes, and concepts in the Infrastructure Optimization Model.

These resource guides are not meant to be used to deploy new IT services or capabilities. Their purpose is to outline the high-level considerations, steps, processes, and Microsoft tools you can use to bring greater efficiency, organization, and profitability to your IT department as you implement those capabilities and services. You can use the information contained in this guide to help you move from the Standardized level to the Rationalized level.

Resource Guide Overview

# Audience

This document is designed for IT professionals who are responsible for planning, deploying, and operating IT systems and data centers, and who want to implement the technology and procedural concepts of the Core Infrastructure Optimization Model.

# Infrastructure Optimization Concept

Microsoft Infrastructure Optimization (IO) is structured around three information technology models: Core Infrastructure Optimization, Application Platform Infrastructure Optimization, and Business Productivity Infrastructure Optimization. Each of these IO models contains four levels of process maturity and capability classifications as logical groupings of requirements for each level of maturity. Core IO focuses on the foundational elements of IT services and components; Application Platform IO focuses on best practices for software development; and Business Productivity IO focuses on the infrastructure required to maximize communication, collaboration, and end-user productivity. The following table highlights the capabilities of each IO model.

|  |  |
| --- | --- |
| **Model** | **Capabilities** |
| Core Infrastructure Optimization Model (Core IOM) | Identity and Access Management |
| Desktop, Device and Server Management |
| Security and Networking |
| Data Protection and Recovery |
| IT and Security Process |
| Application Platform Infrastructure Optimization Model  (AP IOM) | User Experience |
| SOA and Business Process |
| Data Management |
| Development |
| Business Intelligence |
| Business Productivity Infrastructure Optimization Model  (BP IOM) | Collaboration and Communication |
| Enterprise Content Management |
| Business Intelligence |

The Infrastructure Optimization concept helps customers realize dramatic cost savings for their IT infrastructures by moving toward a secure, defined, and highly automated environment. It prescribes capabilities in a logical sequence to help organizations advance up the levels at a measurable and achievable pace. As a basic IT infrastructure matures, security improves from vulnerable to dynamically proactive, and administrative and managerial processes change from highly manual and reactive to highly automated and proactive.

Microsoft and its partners provide the technologies, processes, and procedures to help customers move along the infrastructure optimization path. Processes move from fragmented or nonexistent to optimized and repeatable. Customers' ability to use technology to improve their business agility and to deliver business value increases as they move from the Basic level to the Standardized level, to the Rationalized level, and finally to the Dynamic level. These levels are defined later in this guide.

The Infrastructure Optimization Model has been developed by industry analysts, the Massachusetts Institute of Technology (MIT) Center for Information Systems Research (CISR), and Microsoft's own experiences with its 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 easily be used as the benchmark for technical capability and business value.

The first step in using the model is to evaluate the current maturity level of your IT infrastructure within the model. This helps to determine what capabilities your organization needs, and in what sequence these capabilities should be deployed.

This document focuses on moving from the Standardized level of IT infrastructure and processes to the Rationalized level in the Core Infrastructure Optimization Model. Other resource guides in this series focus on the capabilities necessary to move to the other levels in the Core Infrastructure Optimization Model.

# Core Infrastructure Optimization Capabilities

The Core Infrastructure Optimization Model defines five capabilities that are initial requirements to build a more agile IT infrastructure. These five capabilities are the foundation of each of the maturity levels.

## Identity and Access Management

Describes how customers should manage people and asset identities, how to implement solutions to manage and protect identity data, and how to manage access to resources from corporate mobile users, customers, and/or partners outside of a firewall.

## Desktop, Device and Server Management

Describes how customers should manage desktops, mobile devices, and servers, in addition to how to deploy patches, operating systems, and applications across the network.

## Security and Networking

Describes what customers should consider implementing in their IT infrastructures to help guarantee that information and communication are protected from unauthorized access. Also provides a mechanism to protect the IT infrastructure from denial attacks and viruses, while preserving access to corporate resources.

## Data Protection and Recovery

Provides structured and disciplined backup, storage, and restore management. As information and data stores proliferate, organizations are under increasing pressure to protect information and provide cost-effective and time-efficient recovery when required.

## IT and Security Process

Provides proven best practice guidance on how to cost-effectively design, develop, operate, and support solutions while achieving high reliability, availability, and security. Although rock-solid technology is necessary to meet demands for reliable, available, and highly secure IT services, technology alone is not sufficient; excellence in process and people (skills, roles, and responsibilities) is also needed. This document addresses Security Process and IT Process (ITIL/COBIT-based Management Process) in separate sections.

# Core Infrastructure Optimization Model Levels

In addition to capabilities, the Core Infrastructure Optimization Model defines four optimization levels (Basic, Standardized, Rationalized, and Dynamic) for each capability. The characteristics of these optimization levels are described in the following sections.

## Optimization Level 1: Basic

The Basic IT infrastructure is characterized by manual, localized processes; minimal central control; and nonexistent or unenforced IT policies and standards for security, backup, image management and deployment, compliance, and other common IT practices. Overall health of applications and services is unknown due to a lack of tools and resources. Generally, all patches, software deployments, and services are provided manually.

## Optimization Level 2: Standardized

The Standardized infrastructure introduces controls through the use of standards and policies to manage desktops and servers; to control the way machines are introduced into the network; and by using Active Directory® directory service to manage resources, security policies, and access control. Customers in a Standardized state have realized the value of basic standards and some policies, yet still have room to improve. Generally, all patches, software deployments, and desktop service are provided through medium touch with medium to high cost. These organizations have a reasonable inventory of hardware and software and are beginning to manage licenses. Security measures are improved through a locked-down perimeter, but internal security may still be a risk.

## Optimization 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 been optimized to begin playing a large role in supporting and expanding the business. Security is very proactive, and responding to threats and challenges is rapid and controlled. The use of zero touch deployment helps minimize cost, the time to deploy, and technical challenges. The number of images is minimal, and the process for managing desktops is very low touch. These customers have a clear inventory of hardware and software and only purchase the licenses and computers they need. Security is extremely proactive with strict policies and control, from the desktop to server to firewall to extranet.

## Optimization Level 4: Dynamic

Customers with a Dynamic infrastructure are fully aware of the strategic value that their infrastructure provides in helping them run their business efficiently and staying ahead of competitors. Costs are fully controlled; there is 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 business needs. Additional investments in technology yield specific, rapid, and 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 infrastructure organization to automate processes, thus helping improve reliability, lower costs, and increase service levels.

# Core Infrastructure Optimization Capability Overview

The following image lists the basic requirements for each capability to advance through the optimization levels.

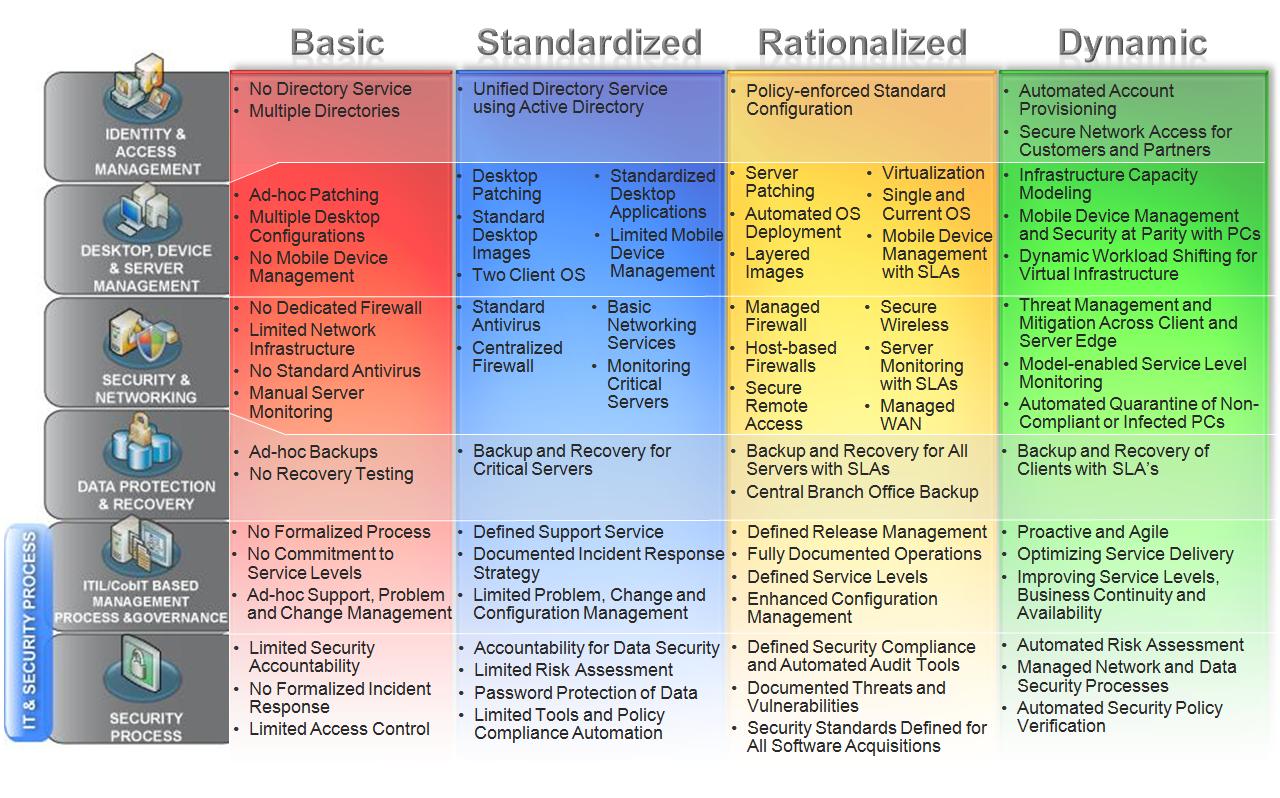


Figure 1. Capability requirements of each optimization level

For more information, including customer case studies and business value information, visit <http://www.microsoft.com/technet/infrastructure/default.mspx>.

## Self Assessment

Microsoft has developed a self-assessment tool that you can use to determine your current optimization level. We recommend that you use this tool before proceeding with this guide. The tool is based on the material presented in this guide. To access the self-assessment tool, visit: <http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx>.

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Rationalized level and can proceed to the Dynamic level in Core Infrastructure Optimization. You can print this section as a scorecard for determining which requirements and attributes you need to implement in your organization.

### Capability: Identity and Access Management

The Rationalized level of optimization requires a directory-based tool to centrally administer configurations and security on 80 percent or more desktops in your organization.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

For more details, see [Centralized Directory-based Configuration and Security](#_Centralized_Directory_Based) in this document, or visit the following Web sites:

* [Windows Server 2003 Active Directory Technology Center](http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx)
* [Windows® XP Security Guide](http://go.microsoft.com/fwlink/?linkid=14839)
* [Windows Vista Security Guide](http://go.microsoft.com/fwlink/?linkid=74027)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true)
* [Microsoft Operations Framework Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Medium Business Solution for Management and Security using Active Directory Group Policy](http://www.microsoft.com/downloads/details.aspx?FamilyId=BB534B41-B413-4483-9097-879F5CAFE2DC&displaylang=en)

Additional information is available at [Medium Business Solution for Client Configuration](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/cc/mit_cc.mspx).

### Capability: Desktop, Device and Server Management

The Rationalized level of optimization requires that your organization has procedures and tools in place to automate operating system deployment, track desktop assets, test application compatibility, streamline desktop deployment with a layered-image approach, automate server patch management, provide secure access to mobile devices, and explore server consolidation through virtualization technologies.

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| An automated software distribution solution for operating system deployment |  |  |
| Attributes:   * Identified tools and technologies required to enable automated operating system deployment. * Performed necessary pre-deployment tasks for application compatibility and packaging, infrastructure remediation, imaging, user-state migration, and desktop security. * Tested and validated Zero Touch Installation in a lab environment and pilot program. * Performed automated OS deployment to end users. | | |

For more details, see [Automated Operating System Distribution](#_Automated_Patch_Distribution) in this document, or visit the following Web sites:

* [Microsoft TechNet Desktop Deployment Center](http://www.microsoft.com/technet/desktopdeployment/default.mspx)
* [Microsoft TechNet Systems Management Server TechCenter](http://www.microsoft.com/technet/sms/default.mspx)
* [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Automated tracking of hardware and software assets of 80 percent or more of your desktops |  |  |
| Attributes:   * Deployed tools and procedures to automate desktop asset inventory. * Implemented procedures and technologies to automate application and operating system deployment * Implemented tools and procedures to perform and analyze software usage tracking reporting. * Implemented best practice automated software update management. * Deployed tools and procedures to monitor desktop system status, including product compliance and system status monitoring. | | |

For more details, see [Automated Tracking of Hardware and Software for Desktops](#_Automated_Tracking_of) in this document, or visit the following Web sites:

* [Microsoft TechNet Systems Management Server TechCenter](http://www.microsoft.com/technet/sms/default.mspx)
* [Microsoft TechNet Update Management TechCenter](http://www.microsoft.com/technet/updatemanagement/default.mspx)
* [Microsoft TechNet Desktop Deployment Center](http://www.microsoft.com/technet/desktopdeployment/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Eighty percent or more of your desktops running one of the two most recent operating system versions |  |  |
| Attributes:   * Inventoried existing production operating systems. * Determined new computer and refresh strategies in order to phase out older operating systems. * Deployed two most recent operating system versions to at least 80 percent of all desktops. | | |

For more details, see [Latest Two OS Versions and Service Packs on Desktops](#_Requirement:_Latest_Two) in this document, or visit the following Web sites:

* [Microsoft TechNet Desktop Deployment Center](http://www.microsoft.com/technet/desktopdeployment/default.mspx)
* [Microsoft TechNet Systems Management Server TechCenter](http://www.microsoft.com/technet/sms/default.mspx)
* [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx)
* [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Eighty percent or more of your desktops running Microsoft Office 2003 or the 2007 Microsoft Office system |  |  |
| Attributes:   * Evaluated the latest versions of Office and defined plan to consolidate Office versions on production workstations. * Deployed latest versions of Office to desktops. * Defined plan for managing Office configurations | | |

For more details, see [Latest Versions of Microsoft Office on Desktops](#_Latest_Version_of) in this document, or visit the following Web sites:

* [Microsoft TechNet Office System TechCenter](http://www.microsoft.com/technet/prodtechnol/office/default.mspx)
* [Office Resource Kit](http://technet2.microsoft.com/Office/en-us/library/9df1c7d2-30a9-47bb-a3b2-5166b394fbf51033.mspx)
* [Microsoft TechNet Desktop Deployment Center](http://www.microsoft.com/technet/desktopdeployment/default.mspx)
* [Microsoft TechNet Systems Management Server TechCenter](http://www.microsoft.com/technet/sms/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Tests and certifies application compatibility on 80 percent of new or updated applications before deploying them to desktops |  |  |
| Attributes:   * Collected and analyzed the application inventory in your organization to build your application portfolio. * Implemented standard testing of your mitigation strategies to create your application mitigation packages. * Implemented standard processes to resolve any outstanding compatibility issues to report compatibility mitigation to management. * Implemented automated deployment of all compatibility mitigation packages. | | |

For more details, see [Compatibility Testing and Certification of Software Distributions](#_Requirement:_Compatibility_Testing) in this document, or visit the following Web sites:

* [Microsoft Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx)
* [BDD 2007 Application Compatibility Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppCompact_1b.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Patch management solution for 80 percent or more of your servers |  |  |
| Attributes:   * Implemented process and tools to inventory hardware and software assets. * Implemented process and tools to scan servers for software updates. * Established a process to automatically identify available patches. * Established standard testing for every patch. * Implemented patch distribution software. | | |

For more details, see [Patch Management for Servers](#_Patch_Management_for) in this document, or visit the following Web sites:

* [Update Management Solution Center on Microsoft TechNet](http://www.microsoft.com/technet/updatemanagement/default.mspx)
* [Patch Management Solution Accelerator content](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/default.mspx)
* [Medium Business Solution for Patch Management](http://www.microsoft.com/technet/solutionaccelerators/smbiz/mits/pm/mit_pm.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Secured and guaranteed way to verify secure communications between your corporate network and mobile devices |  |  |
| Attributes:   * Inventoried mobile devices connecting to your network. * Determined a communication security strategy appropriate for your needs. * Implemented mobile device authentication to all connected devices. | | |

For more details, see [Guaranteed Secure Communications with Mobile Devices](#_Guaranteed_Secure_Communications) in this document, or visit the following Web sites:

* [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx)
* [Windows Mobile Solutions Providers](http://www.microsoft.com/windowsmobile/business/solutions/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Access provided to Web applications via WAP or HTTP for mobile devices |  |  |
| Attributes:   * Inventoried mobile devices connecting to your network and Web applications currently consumed or potentially consumed by mobile device users. * Developed and implemented a strategy to optimize Web applications for mobile device users, update mobile device hardware, or both. | | |

For more details, see [Access to Web Applications Using WAP or HTTP for Mobile Devices](#_Requirement:_Access_to) in this document, or visit the following Web sites:

* [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx)
* [Windows Mobile Solutions Providers](http://www.microsoft.com/windowsmobile/business/solutions/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Planning for server consolidation with virtualization |  |  |
| Attributes:   * Inventoried all IT services and LOB applications in your organization, including performance and traffic data. * Developed a plan to consolidate server infrastructure by implementing virtual machine technologies. | | |

For more details, see [Server Consolidation with Virtualization](#_Server_Consolidation_and) in this document, or visit the following Web sites:

* [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx)
* [Windows Server System™ Architecture Virtual Environments for Development and Test](http://www.microsoft.com/technet/solutionaccelerators/wssra/ve/default.mspx)
* [Virtual Server Technology Center on Microsoft TechNet](http://www.microsoft.com/technet/prodtechnol/virtualserver/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Implemented a layered-image strategy for managing your desktop images |  |  |
| Attributes:   * Inventoried and rationalized the current set of managed desktop images in your organization. * Developed and implemented a strategy to consolidate desktop images by using thin or hybrid layered imaging for desktop deployment. | | |

For more details, see [Layered Imaging for Desktops](#_Layered_Imaging_for) in this document, or visit the following Web sites:

* [Business Desktop Deployment (BDD) 2007 Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx)
* [BDD 2007 Application Management Featur](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppMgmt.mspx)[e Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppMgmt.mspx)
* [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625)

### Capability: Security and Networking

The Rationalized level of optimization requires that your organization has standard antivirus software installed on client computers, a centralized perimeter firewall, basic networking services, and availability monitoring for critical servers.

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Policy-managed firewall on 80 percent or more of your servers and desktops |  |  |
| Attributes:   * Inventoried your desktop and server computers to identify which hardware currently has host-based firewall technologies. * Deployed host-based firewall technology to hardware lacking firewall capabilities or updated servers to Windows Server 2003 SP1 or later. * Established policy enforcement to ensure host-based firewalls are always enabled and cannot be disabled. | | |

For more details, see [Policy-managed Firewalls on Servers and Desktops](#_Policy_Managed_Firewall) in this document, or visit the following Web sites:

* [Windows Firewall TechCenter](http://www.microsoft.com/technet/network/wf/default.mspx)
* [Best Practices for Managing Windows Firewall](http://technet2.microsoft.com/WindowsServer/en/library/985a4443-4db7-4cce-b523-fd7414fe01271033.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Secure remote access to internal resources and line-of-business (LOB) applications beyond e-mail (that is, VPN and/or Terminal Services) |  |  |
| Attributes:   * Evaluated remote access requirements for remote clients and branch offices. * Designed and implemented secure virtual private network or similar services to remote clients and branch office. | | |

For more details, see [Secure Remote Access to Internal Resources and LOB Applications](#_Requirement:_Secure_Remote) in this document, or visit the following Web sites:

* [Virtual Private Networks Web site on Microsoft TechNet](http://www.microsoft.com/technet/network/vpn/default.mspx)
* [Windows Server System Reference Architecture (WSSRA) Remote Access Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/remoteaccessservices/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Secured and guaranteed way to verify communication between critical servers, such as domain controllers and e-mail servers |  |  |
| Attributes:   * Assessed the current state of network infrastructure affected by Internet Protocol security (IPsec). * Identified organizational requirements to ensure secured and guaranteed communication between servers, including regulation and compliance impacts. * Developed and implemented a plan across the organization using IPsec to meet defined requirements | | |

For more details, see [Secured and Guaranteed Communication Between Servers](#_Secured_and_Guaranteed) in this document, or visit the following Web sites:

* [Server and Domain Isolation Using IPsec and Group Policy Guide on Microsoft TechNet](Server%20and%20Domain%20Isolation%20Using%20IPsec%20and%20Group%20Policy)
* [Determining Your IPsec Need in the Windows Server 2003 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=76094&clcid=0x409)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Monitoring and service level reporting for 80 percent or more of your servers to ensure a consistent and reliable user experience |  |  |
| Attributes:   * Defined your organization’s IT services in a service catalog. * Determined the baseline or current service levels for defined services. * Defined service levels appropriate for your organization and determined a plan for automating service level monitoring. * Implemented an automated availability monitoring solution. | | |

For more details, see [Service Level Agreement Monitoring and Reporting for Servers](#_Service_Level_Agreement) in this document, or visit the following Web sites:

* [Microsoft Operations Framework Service Monitoring and Control](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsmc.mspx)
* [Microsoft Operations Framework Availability Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx)
* [Microsoft Operations Framework Service Level Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx)
* [Microsoft TechNet Operations Manager 2005 TechCenter](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx)
* [System Center Operations Manager 2007 on Microsoft TechNet](http://www.microsoft.com/technet/opsmgr/opsmgr2007_default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Providing a secured communication mechanism for presence |  |  |
| Attributes:   * Assessed any current unmanaged methods used for presence and instant communication. * Created a requirements specification for presence and instant messaging, aligning to industry or local regulations and policies. * Evaluated presence and instant technology and created plan to implement your selected solution. * Implemented presence at minimum through managed instant messaging and optionally through collaboration and e-mail infrastructure. | | |

For more details, see [Secure Communication Mechanism for Presence](#_Requirement:_Secure_Communication) in this document, or visit the following Web sites:

* [Microsoft Office Live Communications Server TechCenter](http://www.microsoft.com/technet/prodtechnol/office/livecomm/default.mspx)
* [Office Communicator 2005 Resource Center](http://office.microsoft.com/en-us/help/HA011992481033.aspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Deployed a secure wireless network using Active Directory and IAS/RADIUS for authentication and authorization |  |  |
| Attributes:   * Identified current wireless access and related topologies. * Evaluated wireless technologies, protocols, and standards. * Developed and implemented plans for secure wireless authentication infrastructure. | | |

For more details, see [Active Directory and IAS/RADIUS for Wireless Network Authentication and Authorization](#_Requirement:_Active_Directory) in this document, or visit the following Web sites:

* [Securing Wireless LANs with Certificate Services Guide](http://go.microsoft.com/fwlink/?LinkId=14843)
* [Securing Wireless LANs with PEAP and Passwords](http://go.microsoft.com/fwlink/?linkid=23459)
* [Microsoft Operations Framework Service Monitoring and Control](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsmc.mspx)
* [Microsoft Operations Framework Availability Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Centrally managed certificate services infrastructure (PKI) |  |  |
| Attributes:   * Performed a network discovery to inventory all components. * Identified people, process, and technology design considerations for the certification authority and public key infrastructure (PKI). * Created a detailed deployment plan to enable the PKI. * Implemented PKI deployment plan. | | |

For more details, see [Centrally Managed Certificate Services](#_Requirement:_Centrally_Managed) in this document, or visit the following Web sites:

* [Windows Server System Reference Architecture Certificate Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/certificateservices/default.mspx)
* [Windows Server 2003 Technical Library: Designing a Public Key Infrastructure](http://technet2.microsoft.com/WindowsServer/en/library/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b1033.mspx)
* [Securing Wireless LANs with Certificate Services Guide](http://go.microsoft.com/fwlink/?LinkId=14843)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Proactively managing bandwidth to branch offices |  |  |
| Attributes:   * Identified and documented branch office topology. * Created requirement specification based on the needs of all branch office types. * Created a plan and architecture for branch office service consolidation and identified performance thresholds for reexamination of branch office WAN requirements. * Implemented plan to optimize branch office services against WAN link limitations. | | |

For more details, see [Proactively Managed Bandwidth to Branch Offices](#_Requirement:_Proactively_Managed) in this document, or visit the following Web sites:

* [Branch Office Infrastructure Solution for Microsoft Windows Server 2003 Release 2 (BOIS R2)](http://www.microsoft.com/technet/solutionaccelerators/branch/default.mspx)
* [Solution Accelerator for Consolidating and Migrating LOB Applications](http://go.microsoft.com/fwlink/?LinkId=47191)
* [Mixed Workload Consolidation Guide](http://go.microsoft.com/fwlink/?LinkId=46571)

### Capability: Data Protection and Recovery

The Rationalized level of optimization requires that your organization has procedures and tools in place to manage backup and recovery of data on servers and to control centralized backup of branch office data.

|  |  |  |
| --- | --- | --- |
| Requirement: Data Protection and Recovery | Yes | No |
| Centrally managing data backup for your branch offices |  |  |
| Attributes:   * Created a centralized data backup plan and a recovery plan for branch offices in your organization. * Implemented a backup and recovery plan for centralized control of backup and recovery operations, either via network-centralized tools or operational guidelines for local backup and recovery, with defined service levels. | | |

For more details, see [Centrally Managed Data Backup for Branch Offices](#_Centrally_Managed_Data) in this document, or visit the following Web sites:

* [Branch Office Solution Center on Microsoft TechNet](http://www.microsoft.com/technet/branchoffice/default.mspx)
* [Microsoft Data Protection Manager 2006 Planning Guide](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/57145992-e0e0-43be-837c-19a7b3b463c8.mspx)
* [Windows Server System Reference Architecture Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Data Protection and Recovery | Yes | No |
| Service level agreement (SLA) for system backup and restore, and defined recovery times for 80 percent of your servers |  |  |
| Attributes:   * Created a data backup plan and a recovery plan for 80 percent or more of all servers in your organization. * Used drills to test your plans and validate defined recovery times. | | |

For more details, see [Backup, Restore, and Defined Recovery Times for Servers](#_Backup,_Restore,_Defined) in this document, or visit the following Web sites:

* [Windows Server System Reference Architecture Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx)
* [Microsoft Operations Framework Service Level Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx)
* [Microsoft Operations Framework Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx)
* [Microsoft Data Protection Manager](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/default.mspx?mfr=true)

### Capability: Security and ITIL/COBIT-based Management Process

The Rationalized level of optimization requires that your organization has defined procedures for risk management, incident management and response, application testing, problem management, user support, configuration management, and change management.

|  |  |  |
| --- | --- | --- |
| Requirement: Security and ITIL/COBIT-based Management Process | Yes | No |
| Established security processes for two-factor user authentication, standard security review for new software acquisitions, and data classification |  |  |
| Attributes:   * Developed and implemented two-factor identity and access management policies. * Developed a process to manage security requirement testing on all acquired or developed software. * Established a standard and repeatable procedure for classifying sensitive data. | | |

For more details, see [Two-Factor User Authentication, Standard Security Review for New Software Acquisitions, and Data Classification Processes](#_Requirement:_Two-Factor_User) in this document, or visit the following Web sites:

* [The Secure Access Using Smart Cards Planning Guide](http://www.microsoft.com/technet/security/guidance/networksecurity/securesmartcards/default.mspx)
* [ISO/IEC 17799:2005 Code of Practice for Information Security Management](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=)
* [Regulatory Compliance Planning Guide on Microsoft TechNet](http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/default.mspx?mfr=true)
* [Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and ITIL/COBIT-based Management Process | Yes | No |
| Implemented best practices for operating, optimizing, and change processes in your IT organization |  |  |
| Attributes:   * Implemented service level management across IT operations. * Implemented best practice release management. * Optimized network and system administration processes. * Implemented best practice job scheduling. | | |

For more details, see [Operating, Optimizing, and Change Processes](#_Requirement:_Operating,_Optimizing,) in this document, or visit the following Web site:

[Microsoft Operations Framework (MOF) on Microsoft TechNet](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/default.mspx)

## Preparing to Implement Core IO Requirements

The detailed capability and requirement sections of the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide will expose you to the high-level context of the processes and technologies necessary to help implement the requirements of the Core Infrastructure Optimization Model at the Rationalized level. These sections provide contextual detail for areas to focus on, an introduction to processes and technologies, and links to relevant implementation guidance throughout.

Microsoft Core IO requires that directory services are based on Active Directory in Microsoft Windows Server products. Microsoft partner and third-party solutions can be used to meet all requirements in the model if functionality meets defined requirements.

### Phased Approach

Microsoft recommends a phased approach to meeting the requirements of each of the IO capabilities. The four phases are shown in the following graphic.

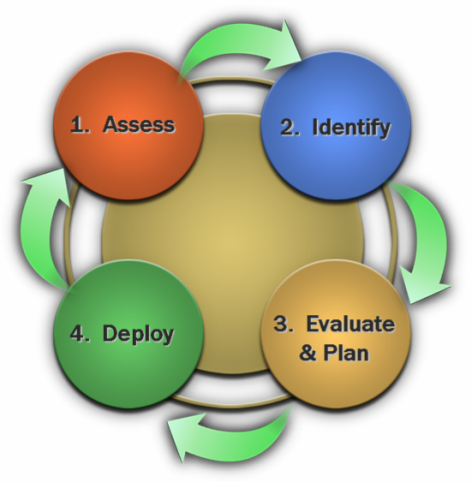


Figure 2. Four phases of the IO capabilities

In the **Assess** phase you determine the current capabilities and resources within your organization.

In the **Identify** phase you determine what you need to accomplish and what capabilities you want to incorporate.

In the **Evaluate and Plan** phase you determine what you need to do to implement the capabilities outlined in the Identify phase.

In the **Deploy** phase you execute the plan that you built in the prior phase.

### Solution Currency

The detailed Capability and Requirement sections of the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide highlight guidance and technologies available from Microsoft as of the release date of the document. We expect that these technologies will evolve, as will the accompanying guidance. Please visit [Microsoft TechNet](http://www.microsoft.com/technet) regularly for any updates to products and capabilities referred to in this document.

### Implementation Services

Implementation services for the projects outlined in this document are provided by Microsoft partners and Microsoft Services. For assistance implementing Core Infrastructure Optimization projects highlighted in the Core Infrastructure Optimization Implementer Resource guides, contact a [Microsoft partner near you](http://directory.microsoft.com/mprd/default.aspx) or visit the [Microsoft Services Web site](http://www.microsoft.com/services/microsoftservices/default.mspx) for more details.

Capability: Identity and Access Management

# Introduction

Identity and Access Management is a Core Infrastructure Optimization capability and the foundation for implementing many capabilities in the Infrastructure Optimization Model.

The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Difficult to enforce IT policies required by the organization or regulations  No way to enable a known, stable, and secure state for client PCs  **IT Challenges**  No centralized policy control for identity and access management—implementing broad policy changes requires modification of each identity  Identities are centrally administered, but difficult to manage users and resource settings, configurations | **Projects**  Identify and define configuration standards requiring enforcement  Implement a centralized, directory-based policy solution for administration of desktops, servers, configuration, and security | **Business Benefits**  Enforced, known state of environment  Consistent user experience across PCs based on business role  Easier to modify system and add functionality  Reduced operations and desktop support costs  Reduced user downtime and disruption  **IT Benefits**  Reduced workload due to introduction of role-based administration/group policy  Improved security by implementing policy-based patch management and security lockdown  Profile management allows user system and data recovery |

Ongoing Identity and Access Management focuses on the following capabilities as outlined in the Microsoft Identity and Access Management Series:

* The Foundation for Identity and Access Management
* [Fundamental Concepts](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Fund.mspx)
* [Platform and Infrastructure](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P1Plat.mspx)
* Identity Life-Cycle Management
* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx)
* [Password Management for Intranet and Extranet](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2pass.mspx)
* [Provisioning and Workflow](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

Note that the capabilities outlined above are all key parts of the Identity and Access Management service in any organization. For more information, please see the [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx).

The Rationalized level of Identity and Access Management in the Infrastructure Optimization Model addresses the need for centralized control of configurations and security.

# Requirement: Centralized Directory-based Configuration and Security

## Audience

You should read this section if you do not have a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops.

## Overview

Administrators face increasingly complex challenges in managing their IT infrastructures. You must deliver and maintain customized desktop configurations for many types of workers, including mobile users, information workers, or others assigned to strictly defined tasks, such as data entry. Changes to standard operating system images might be required on an ongoing basis. Security settings and updates must be delivered efficiently to all the computers and devices in the organization. New users need to be productive quickly without costly training. In the event of a computer failure or disaster, service must be restored with a minimum of data loss and interruption.

## Phase 1: Assess

The primary goal of the Assess phase is to examine which tools and procedures you currently have in place to maintain standard security and user configurations. Your current policies may be managed manually or be automated through patch management, required software installation, or inclusion of required configurations in standard disk images. Through these and other activities in the Standardized level, your organization is maintaining a standard foundation; implementation of configuration control will help you move to the Rationalized level of infrastructure optimization.

## Phase 2: Identify

During the Identify phase you examine current configuration standards as executed by configuration management policies, patching, and disk imaging procedures, and then you look beyond current practices to identify the total number of security and configuration controls requiring enforcement. These configurations can be:

* Components required on PCs, such as patches, service packs, or applications.
* Services or applications required to run on PCs, such as desktop firewall or antivirus applications.
* Data access and transfer rules, such as not allowing file transfers in instant messaging applications.

The exercise of defining the configuration and settings as candidates for policy control are the initial steps to configuration management. Configuration management was also covered briefly in the *Core Infrastructure Optimization Implementer Resource Guide Basic to Standardized*. Read more about [Configuration Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcfgmg.mspx) as part of [Microsoft Operations Framework](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/default.mspx).

## Phase 3: Evaluate and Plan

Your goal during the Evaluate and Plan phase is to determine the level of control for identified configuration and security settings. The level of control will vary from having the ability to simply monitor out-of-compliance configuration to actively automating compliance enforcement.

Configuration monitoring tools are available to provide reports for out-of-compliance configuration. In many cases, your organization may want to report on out-of-compliance and then determine the correct course of action to bring the PC back into compliance. For example, if you want to enforce that an application is installed on all PCs, but that application requires drivers that do not exist for certain hardware types in your desktop environment, the best option may be to monitor these out-of-compliance instances and determine the best way to resolve them on an individual basis. The Rationalized level in Core Infrastructure Optimization requires implementation of a directory-based configuration management infrastructure using Group Policy and recommends—but does not require—stand-alone configuration monitoring tools.

### Configuration Monitoring Tools

Microsoft offers two types of tools to monitor configuration compliance. The first type, called Best Practice Analyzers or BPA, contains Microsoft pre-defined best practice settings and reports. There are BPA tools available as free downloads for Microsoft server products: [Microsoft Exchange Server](http://www.microsoft.com/downloads/info.aspx?na=22&p=1&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3ddbab201f-4bee-4943-ac22-e2ddbd258df3%26DisplayLang%3den), [Microsoft Internet Security and Acceleration Server](http://www.microsoft.com/downloads/info.aspx?na=22&p=2&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3dd22ec2b9-4cd3-4bb6-91ec-0829e5f84063%26DisplayLang%3den), and [Microsoft SQL Server](http://www.microsoft.com/downloads/info.aspx?na=22&p=3&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3db352eb1f-d3ca-44ee-893e-9e07339c1f22%26DisplayLang%3den). The second type of configuration monitoring tool enables your organization to define desired configuration settings or rules specific to your organization and monitor compliance. This tool, [Systems Management Server 2003 Desired Configuration Monitoring](http://www.microsoft.com/downloads/details.aspx?FamilyID=a867fc14-daa3-4c2a-9e65-4fbcbec60aaa&DisplayLang=en), is also a free download and enables you to define customized configuration standards for desktops and servers. You use Systems Management Server 2003 Desired Configuration Monitoring to perform compliance audits, and included reports notify you of specific out-of-compliance cases. In addition to these tools, there are a number of software applications available from Microsoft partners to define and manage standard configuration.

### Group Policy in Windows Server

The next stage of control is automated configuration enforcement. A large portion of required configuration and security settings can be defined with standard policies. Group Policy enables you to automate the step to bring many out-of-compliance instances back into compliance.

Group Policy is an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. This infrastructure consists of a Group Policy engine and multiple client-side extensions responsible for writing specific policy settings on target client computers.

### Group Policy and Active Directory

Administrators use Group Policy to define specific configurations for groups of users and computers by creating Group Policy settings. These settings are specified through the Group Policy Object Editor tool and contained in a Group Policy object (GPO), which is in turn linked to Active Directory containers. Group Policy settings are applied to the users and computers in those Active Directory containers. Administrators can configure the user’s work environment once and rely on the system to enforce the policies as defined.

Active Directory organizes objects by sites, domains, and organizational units (OUs). Domains and OUs are organized hierarchically, making the containers and the objects within them easy to manage. The settings defined in a GPO can only be applied when the GPO is linked to one or more of these containers.

By linking GPOs to sites, domains, and OUs, you can implement Group Policy settings for as broad or as narrow a portion of the organization as you want. GPO links affect users and computers in the following ways:

* A GPO linked to a site applies to all users and computers in the site.
* A GPO linked to a domain applies directly to all users and computers in the domain and by inheritance to all users and computers in child OUs. Note that policy is not inherited across domains.
* A GPO linked to an OU applies directly to all users and computers in the OU and by inheritance to all users and computers in child OUs.

The figure below shows how GPOs are applied to sites, domains, and the OUs beneath them.



Figure 3. Applying GPOs

#### Group Policy Capabilities

Through Group Policy, administrators define the policies that determine how applications and operating systems are configured and keep users and systems secure. The following sections describe the key features of Group Policy.

##### Registry-based Policy

The most common and the easiest way to provide policy for an application or operating system component is to implement registry-based policy. With Group Policy you can define registry-based policy settings for applications, the operating system, and its components.

##### Security Settings

Group Policy provides options for administrators to set security options for computers and users within the scope of a GPO. Local computer, domain, and network security settings can be specified. For more information on Group Policy security and settings, see the [Windows Server 2003 Security Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=5&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3d8a2643c1-0685-4d89-b655-521ea6c7b4db%26DisplayLang%3den), [Windows XP Security Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=6&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3d2d3e25bc-f434-4cc6-a5a7-09a8a229f118%26DisplayLang%3den), [Windows Vista Security Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=1&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3da3d1bbed-7f35-4e72-bfb5-b84a526c1565%26DisplayLang%3den), and [Threats and Countermeasures Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=9&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3d1b6acf93-147a-4481-9346-f93a4081eea8%26DisplayLang%3den).

##### Software Restrictions

To defend against viruses, unwanted applications, and attacks on computers running Windows XP, Windows Vista, and Windows Server 2003, Group Policy includes software restriction policies.

##### Software Distribution and Installation

Group Policy can manage application installation, updates, and removal centrally.

##### Computer and User Scripts

Administrators can use scripts to automate tasks at computer startup and shutdown and user logon and logoff.

##### Roaming User Profiles and Redirected Folders

Roaming user profiles provide the ability to store user profiles centrally on a server and load them when a user logs on. As a result, users experience a consistent environment no matter which computers they use.

##### Offline Folders

When a network is unavailable, the Offline Folders feature provides access to network files and folders from a local disk.

##### Internet Explorer Maintenance

Administrators can manage and customize the configuration of Microsoft Internet Explorer® on computers that support Group Policy.

## Phase 4: Deployment

The Deployment phase focuses primarily on defining Group Policy objects with the Object Editor. GPOs should reflect what was identified during the Assess and Identify phases. Operations has been added to this capability and focuses on the Group Policy Management Console and ongoing operations.

Before implementing Group Policy in your organization, we recommend that you become familiar with the [key concepts for Group Policy](http://technet2.microsoft.com/WindowsServer/en/library/6eed436f-5b05-4eaa-9525-c0c429fcf9f61033.mspx), [how to use the Group Policy Object Editor](http://technet2.microsoft.com/WindowsServer/en/library/c1fbfde3-8d94-4d70-aa97-e43afa550c6e1033.mspx), and [how to configure Group Policy settings](http://technet2.microsoft.com/WindowsServer/en/library/018452a7-a290-4cc3-9cc2-30679e8060381033.mspx). See the [Group Policy Overview](http://technet2.microsoft.com/WindowsServer/en/library/6eed436f-5b05-4eaa-9525-c0c429fcf9f61033.mspx?mfr=true) for detailed information on the following Group Policy activities:

* [Open Group Policy Object Editor](http://technet2.microsoft.com/WindowsServer/en/library/4aca5d36-9224-468e-acf8-00462c793e0a1033.mspx)
* [Work with Group Policy Objects](http://technet2.microsoft.com/WindowsServer/en/library/c1fbfde3-8d94-4d70-aa97-e43afa550c6e1033.mspx)
* [Work with Group Policy Object Properties](http://technet2.microsoft.com/WindowsServer/en/library/9584b722-d01f-4942-bae9-0110a155492d1033.mspx)
* [Use Administrative Templates](http://technet2.microsoft.com/WindowsServer/en/library/c9a96203-875b-4fed-be87-ff092cf7bd881033.mspx)
* [Use Startup, Shutdown, Logon, and Logoff Scripts](http://technet2.microsoft.com/WindowsServer/en/library/22cf660f-c165-49e3-b768-2b8898a5684b1033.mspx)
* [Use Group Policy Software Installation](http://technet2.microsoft.com/WindowsServer/en/library/b238ecdb-cda5-402b-9b3d-f232045a30fa1033.mspx)
* [Use Folder Redirection](http://technet2.microsoft.com/WindowsServer/en/library/d0c2fb86-84b6-4815-8482-c20a3fcca9711033.mspx)
* [Configure Group Policy](http://technet2.microsoft.com/WindowsServer/en/library/e946ed52-c8af-482c-a7fb-bb356fc06f4d1033.mspx)
* [Delegate Control of Group Policy](http://technet2.microsoft.com/WindowsServer/en/library/0b921c4b-3932-4ac5-bc48-ac6e08c4cbdf1033.mspx)

## Operations

Operations of Group Policy are characterized by all tasks executed through the Group Policy Management Console (GPMC) user interface. The following list contains links to information on using the Group Policy Management Console:

* [Start Group Policy Management Console](http://technet2.microsoft.com/WindowsServer/en/library/5c4e61cb-b689-4fdf-97c4-ca08520c247d1033.mspx)
* [Create or delete a Group Policy object](http://technet2.microsoft.com/WindowsServer/en/library/4f8dd800-e0e3-44a6-8a4a-d3d34b245fe71033.mspx)
* [Edit a Group Policy object from GPMC](http://technet2.microsoft.com/WindowsServer/en/library/8fb08f1b-0e08-472d-83db-313e2e56e4001033.mspx)
* [Add a forest, site, or domain to the Group Policy Management Console](http://technet2.microsoft.com/WindowsServer/en/library/c97bac7a-0ee3-4508-9331-168ee7e5edc21033.mspx)
* [Search for a Group Policy object](http://technet2.microsoft.com/WindowsServer/en/library/df32c33b-e41c-46de-96b0-cb05b52723251033.mspx)
* [Specify a domain controller](http://technet2.microsoft.com/WindowsServer/en/library/a0786e93-f803-4b4a-b926-723ac4ea110b1033.mspx)
* [View, print, and save a report of Group Policy object settings](http://technet2.microsoft.com/WindowsServer/en/library/7e1bdb8f-f973-4a02-9b1c-b02331c7ccc71033.mspx)
* [Determine resultant set of policy with Group Policy results](http://technet2.microsoft.com/WindowsServer/en/library/df179088-341e-4b60-970a-969ca94688cf1033.mspx)
* [Simulate resultant set of policy using Group Policy modeling](http://technet2.microsoft.com/WindowsServer/en/library/e010dfb2-42fa-4aa9-bb3b-d020217c93021033.mspx)
* [Set Group Policy Management Console user interface options](http://technet2.microsoft.com/WindowsServer/en/library/91b95f32-ffae-4224-8cf9-c929d97b9a9c1033.mspx)
* [Back Up, Restore, Copy, and Import](http://technet2.microsoft.com/WindowsServer/en/library/9397905a-258c-45f6-a62c-1bc6db155e531033.mspx)
* [Control Group Policy Object scope](http://technet2.microsoft.com/WindowsServer/en/library/b48ad46a-d7c4-4cc6-b975-fadc501328311033.mspx)
* [Delegate Group Policy tasks](http://technet2.microsoft.com/WindowsServer/en/library/52c40c95-b89a-4317-a340-6f4cfb358c5b1033.mspx)
* [Use script and command-line methods](http://technet2.microsoft.com/WindowsServer/en/library/1f465485-f6ac-46bb-9cd4-b1e8c30958c01033.mspx)

## Further Information

For more information on Group Policy, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “Group Policy.”

To see how Microsoft manages Group Policy, go to <http://www.microsoft.com/technet/itshowcase/content/grppolobjectmgmt.mspx>.

## Checkpoint: Centralized Directory-based Configuration and Security

|  |  |
| --- | --- |
| X | **Requirements** |
|  | Identified which configurations should be monitored or enforced. |
|  | Selected tools for monitoring and enforcing configuration compliance. |
|  | Defined Group Policy objects for settings managed through Group Policy. |
|  | Implemented Group Policy Management Console to manage Group Policy objects. |
|  | Applied Group Policy to at least 80 percent of your desktops. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Centralized Directory-based Configuration and Security capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for configuration and security management.

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device).

Capability: Desktop, Device and Server Management

# Introduction

Desktop, Device and Server Management is the second Core Infrastructure Optimization capability. The following table describes the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Desktop, Device and Server Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Little protection from unauthorized mobile network access  Limited security options for mobile e-mail  Inability to delegate standard mobility-related support incidents to help desk  **IT Challenges**  Deployments are partially manual and PCs are exposed to attacks or virus infections  Not using automated tools for desktop testing, deployment, and support  Inaccurate knowledge of hardware, software, and desktops increases maintenance costs  Securing servers, PCs, and mobile devices from wired or wireless networks with varying security levels | **Projects**  Automate OS distribution and installation  Automate asset life-cycle management of hardware and software  Install latest two OS versions on desktops  Implement standard compatibility testing and certification of new software  Extend automated patch management to servers  Guarantee secure communications with mobile devices  Provide access to Web applications via WAP or HTTP  Begin using virtualization to consolidate servers  Implement a layered-image approach for desktop deployment | **Business Benefits**  Mobile, secure, centrally managed desktop environment  Reduced user downtime by maintaining patch and operating system updates  Users spend less time with first-line support, resulting from application testing  Highly automated IT services lead to lower costs and improved consistency  **IT Benefits**  Automated deployment of new desktops, desktop rebuilds, and user migrations  More effective desktop security  Consistent security and stability of desktop and mobile environments inside and outside the organizational firewall |

The Rationalized level of optimization requires that your organization has procedures and tools in place to improve automation and flexibility of desktop, server, and device management tasks, while beginning to incorporate new technologies for virtualization and mobility.

# Requirement: Automated Operating System Distribution

## Audience

You should read this section if you do not have an automated software distribution solution for operating system (OS) deployment.

## Overview

In the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide you read about defining and deploying standard images for desktops. To move from the Standardized level to the Rationalized level, you need to automate the deployment of your operating systems to desktops in your organization.

## Phase 1: Assess

The goal of the Assess phase is to examine the current procedures in the organization used to deploy disk images to desktops. The Standardized level assumes that tools and procedures are already in place to perform fully functional image deployment to desktop and laptop computers with minimal interaction at the targeted computer; *fully functional* is defined as installing appropriate applications, drivers, language packs, and updates as well as migration of any existing user state during a deployment sequence. Review Lite Touch Installation (LTI) concepts in the Solution Accelerator for Business Desktop Deployment (BDD) 2007 [Deployment Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/deftgs_3.mspx) for more details.

## Phase 2: Identify

The objective in moving to the Rationalized level is to completely automate existing desktop deployment procedures, enabling a Zero Touch Installation (ZTI) of desktop images, role-based applications, required drivers, language packs, updates, and migration of user state without any interaction at the targeted computer. In this phase, you should identify what is necessary to enable ZTI in your desktop environment.

[BDD 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx) is the recommended resource for identifying deployment options and end-to-end planning of deployment projects. BDD 2007 provides guidance for [Zero Touch Installation (ZTI)](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ZeroTouch_3.mspx) using [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/sms/default.mspx) with the Operating System Deployment Feature Pack.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase requires you to take into account all steps needed prior to performing fully automated deployments. Evaluating and planning for a Zero Touch deployment differs from most other themes in that it requires many action items typically associated with a Deploy phase. In order to successfully deploy to desktops, there are several required steps prior to kicking off an image installation. BDD 2007 outlines these steps as Feature Team Guides; they include:

* Application Compatibility
* Infrastructure Remediation
* Application Management
* Computer Imaging System
* User State Migration
* Securing the Desktop

### Application Compatibility

Application compatibility is often the initial action to prepare for approved desktop deployment projects. In the Application Compatibility step, your organization should:

* Collect and analyze the application inventory in your organization to build your application portfolio.
* Test your mitigation strategies to create your application mitigation packages.
* Resolve any outstanding compatibility issues to report compatibility mitigation to management.
* Deploy compatibility mitigation packages with core application deployment or after core application deployment.

See the [Application Compatibility Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppCompact_1b.mspx) in BDD 2007 for more details.

### Infrastructure Remediation

Understanding the network environment is critical for any deployment project. As part of your planning and preparation, you must understand the current status of your organization's environment, identify other sources of change that may affect the project, and develop a risk-mitigation approach to the changes before incorporating them. In the Infrastructure Remediation step, your organization should:

* Inventory hardware assets for centralized management and research of gathered data. Organizations may consider Systems Management Server 2003, [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625), or the Application Compatibility Toolkit to help inventory client hardware and devices on a network.
* Optimize the infrastructure for deployment of new operating systems and applications.
* Employ technologies to provide for accurate and timely infrastructure-management information.

See the [Infrastructure Remediation Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/InfraRmdtn_1.mspx) in BDD 2007 for more details.

### Application Management

Application management focuses on the tasks required to package applications and enable scripted installation. Application packaging results in consistent, reliable, and more serviceable application deployment. In the Application Management step as defined by BDD 2007, your organization should:

* Identify, inventory, and prioritize core and supplemental applications.
* Develop and test deployment packages.
* Add applications to the deployment sequence.

See the [Application Management Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppMgmt_3.mspx) in BDD 2007 for more details.

### Computer Imaging System

Standard desktop imaging is covered in the *Core Infrastructure Optimization Implementer Resource Guide: Basic to Standardized*. The Standardized level assumes that your organization already employs a standard and tested image for provisioning new users, upgrading operating systems, or refreshing corrupted PCs. The Rationalized level requires a layered-image approach using thin OS images and adding the drivers, updates, language packs, and applications as part of the deployment sequence. See the [Layered Imaging for Desktops](#_Identity_Validation,_Data) requirement as part of the Rationalized level.

### User State Migration

Although User State Migration is a deployment preparation step that should be tested prior to the actual image deployment, it occurs during the deployment sequence. User state is the combination of users' data files and their operating system and application settings. Settings include items such as screen saver preferences, My Documents, Web browser favorites, Office Outlook data, and so on. Migrating users' data files and settings means that those users will have minimal interruption after the deployment process. In the User State Migration step, your organization should:

* Capture and store the user data and application information.
* Build the new desktop and install the company-standard image.
* Restore the user data and application information to the new desktop.

See the [User State Migration Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/UserState_2.mspx) in BDD 2007 for more details.

### Securing the Desktop

For most organizations, securing the computing environment is the highest priority of the IT department. When deploying new operating systems or computers, making sure that the new deployments are at least as secure as the current environment is critical. In fact, any process for deploying new computers must include deploying secure systems. By using constantly updated baselines and images, you can keep the environment secure while still allowing quick deployment of new workstations. When securing the desktop for deployment, your organization should:

* Choose and enable the security configuration of your desktops.
* Manage security updates.
* Maintain desktop security.

See the [Security Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/SecFea_2.mspx) in BDD 2007 for more details or read the [Windows XP Security Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=6&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3d2d3e25bc-f434-4cc6-a5a7-09a8a229f118%26DisplayLang%3den) and the [Windows Vista Security Guide](http://www.microsoft.com/downloads/info.aspx?na=22&p=1&SrcDisplayLang=en&SrcCategoryId=&SrcFamilyId=&u=%2fdownloads%2fdetails.aspx%3fFamilyID%3da3d1bbed-7f35-4e72-bfb5-b84a526c1565%26DisplayLang%3den).

## Phase 4: Deploy

After your organization has gone through all of the steps required for pre-deployment, you are ready to start testing and deploying desktop images. All of the pre-deployment steps mentioned above are necessary for a Lite Touch Installation (LTI) or Zero Touch Installation (ZTI). See the [Zero Touch Installation Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ZeroTouch_3.mspx) in BDD 2007 for more details. The following table highlights the differences you need to consider when upgrading from Lite Touch to Zero Touch deployment.

|  |  |
| --- | --- |
| LTI Deployment | ZTI with SMS 2003 Deployment |
| Provides configuration settings that are common to a group of target computers. | Provides all necessary configuration settings for each target computer. |
| Requires less up-front configuration time. | Requires more up-front configuration time. |
| Can be used with slow-speed connections or in instances where no network connectivity exists. | Requires a high-speed, persistent connection. |
| Requires little or no infrastructure to support deployment. | Requires an infrastructure sufficient to deploy operating system images by using SMS 2003 OS Deployment (OSD) Feature Pack. |
| Supports deployment over the network or locally. | Supports only network deployments. |
| Target computers are not required to be managed by SMS 2003 (or other software management tools). | Target computers must be managed by SMS 2003. |
| Supports security policies where automatic software installation is prohibited. | Supports only security where automatic software installation is allowed. |

A BDD 2007 Zero Touch Installation process performs the following tasks:

* Collects hardware and software inventory information by using SMS 2003 with Service Pack 2 (SP2).
* Migrates existing user profile information by using User State Migration Tool (USMT) version 3.0.
* Configures Windows Deployment Services to start the Windows Preinstallation Environment (Windows PE).
* Installs an operating system image on target computers automatically by using the SMS OSD Feature Pack and the deployments scripts for ZTI.
* Optionally, monitors the deployment process by using Microsoft Operations Manager (MOM) 2005 and Zero Touch Installation Management Pack.
* When replacing or refreshing a computer, copies existing user data and preferences.
* Optionally, creates a backup image of the user computer to a network deployment server.
* When used for new users and replacement scenarios, repartitions and formats the existing primary hard drive.
* Dynamically installs applications that are specific to the target computer.
* Automatically installs previously packaged software specific to the user of the target computer.
* When replacing or refreshing a computer, restores the user data and preferences.

All steps and process should be thoroughly tested and validated in a pre-production lab environment and pilot program prior to being implemented into production.

BDD 2007 Zero Touch Installation is built and tested for Systems Management Server (SMS) 2003 with the Operating System Deployment Feature Pack. If your organization is using another technology for operating system deployment, it will require functionality to enable zero touch image installation for new users, computer replacements, and refreshes to meet the requirement of the Rationalized level. The additional requirement of the Rationalized level for layered imaging will also require a task sequencing mechanism used for pre- and post-deployment configuration.

## Further Information

For more information on automating OS distribution, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “OS Deployment” or “Zero Touch Installation.”

To see how Microsoft uses SMS for OS distribution, go to <http://www.microsoft.com/technet/desktopdeployment/depprocess/default.mspx>.

## Checkpoint: Automated Operating System Distribution

|  |  |
| --- | --- |
| X | Requirements |
|  | Identified tools and technologies required to enable automated operating system deployment. |
|  | Performed necessary pre-deployment tasks for application compatibility and packaging, infrastructure remediation, imaging, user-state migration, and desktop security. |
|  | Tested and validated Zero Touch Installation in a lab environment and pilot program. |
|  | Performed automated OS deployment to end users. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Automated Operating System Distribution capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for automated OS deployment in the [Solution Accelerator for Business Desktop Deployment 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_1).

# Requirement: Automated Tracking of Hardware and Software for Desktops

## Audience

You should read this section if you do not have automated tracking of hardware and software assets on 80 percent or more of your desktops.

## Overview

Automated tracking of hardware and software assets addresses and resolves change and configuration needs. By understanding the installed application base and its usage, applying automation helps lower software costs and helps improve configuration compliance. As hardware and software assets comprise an increasing portion of the IT budget, organizations are becoming more focused on finding ways to reduce these costs while continuing to stay compliant with licensing policies.

## Phase 1: Assess

In the Assess phase, you are looking for what processes and tools are currently in place to help automate hardware and software tracking or asset life-cycle management. At the Standardized level, the Infrastructure Optimization Model assumes that your organization has implemented some form of configuration management and incorporates best practices and automation for software update management. See the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* for more details. If your organization currently has systems management software managing the majority of your desktops or an automated configuration management database in place, your organization most likely has the software available to implement automated tracking of assets as defined in the Infrastructure Optimization Model.

## Phase 2: Identify

The goal of the Identify phase is to define what is necessary to expand your current capabilities in order to achieve automated tracking of desktop assets. The *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide includes guidance for tracking hardware and software for mobile devices, desktop patch management, and general configuration management required for moving to the Standardized level. These principles can be extended and applied to all IT assets in your organization. The following attributes are the basic high-level requirements for Automated Tracking of Hardware and Software for Desktops as defined by the Infrastructure Optimization Model:

* Asset Inventory
* Application and Operating System Deployment
* Software Usage Tracking
* Security Patch Management
* System Status Monitoring

At the Standardized level, tools to automate asset inventory are required as part of the patching process, and software update or patch management itself is also a requirement at the Standardized level. Automated tracking of desktop assets then only introduces requirements to automate deployment of applications and operating systems, track usage, and report system status. The Rationalized level requires that all of these tasks are integrated into a common process methodology and toolset. The Evaluate and Plan phase will discuss the specific requirements and recommended tools to implement automated deployment, usage tracking, and system status reporting.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase identifies specific requirements needed to implement Automated Tracking of Hardware and Software Assets. The recommended solution for automating and integrating these tasks is [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/sms/default.mspx), and this requirement will focus on how SMS 2003 can be used. Alternatively, there are tools available from Microsoft’s partners to enable the concepts and requirements discussed for automated tracking of hardware and software assets.

System Center Configuration Manager 2007 is available as a beta release at the time of this publication. As the next version of a change and configuration management solution from Microsoft, it will add features for desired configuration management, integrated operating system deployment, network access protection for non-compliant computers, and improved mobile device support.

### Asset Inventory

Unless you have a baseline inventory of hardware and software assets in your organization, you have very little chance of effectively managing those assets. Often hardware and software can be added or removed without appropriate authorization or using defined acquisition workflows.

There are three primary solutions available from Microsoft that generate an inventory of hardware and software applications. SMS 2003 has built-in functionality to generate detailed hardware and software inventories. The Microsoft [Application Compatibility Toolkit (ACT)](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) is a free tool that can also generate detailed software and hardware inventories using an agent provided with the toolkit. [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625) is a free tool that provides an agent-less inventory of computers across networks.

For more information on SMS 2003 hardware and software inventory, go to <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx>.

For more information on the Application Compatibility Toolkit, go to <http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx>.

### Application and Operating System Deployment

Automated deployment of applications and operating systems along with usage tracking are the core attributes of automated tracking of desktop assets. This section briefly discusses application and operating system deployment.

#### Application Deployment

The [Automated Operating System Distribution](#_Requirement:_Automated_Operating) requirement discussed how applications are packaged for scriptable installation. Packaged applications can be deployed to desktops using software distribution technologies, such as SMS 2003, or via policy enforcement mechanisms, such as Group Policy in Windows Server 2003.

Automated application deployment eliminates the inefficient process of providing CD, DVD, or USB media and installation instructions to end users. By using deployment automation, desktops can successfully install applications remotely with minimal chance for user error. Automated deployment allows you to define and control how and when programs run on desktops.

For more information on how SMS 2003 automates application deployment (recommended), see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan47zc.mspx>.

For more information on how software is installed using Group Policy in Windows Server 2003, see <http://technet2.microsoft.com/WindowsServer/en/library/b238ecdb-cda5-402b-9b3d-f232045a30fa1033.mspx>

#### Operating System Deployment

Automated operating system deployment using Zero Touch Installation is discussed in the [Automated Operating System Distribution](#_Requirement:_Automated_Operating) requirement for the Rationalized level. The recommended approach uses the SMS 2003 Operating System Deployment Feature Pack to enabled fully automated desktop deployment.

### Software Usage Tracking

Software usage tracking or software metering allows you to monitor program usage on desktops. By using SMS 2003 software metering, you can collect data about software usage in your organization. Software metering data can be summarized to produce reports to help you monitor licensing compliance and plan software purchases in your organization. Software metering collects detailed information about the programs that you choose to monitor. This includes information about program usage, program users, the program start time, and the length of time it is used. The following diagram shows how the Software Metering feature in SMS 2003 captures and reports software usage information to a central site.

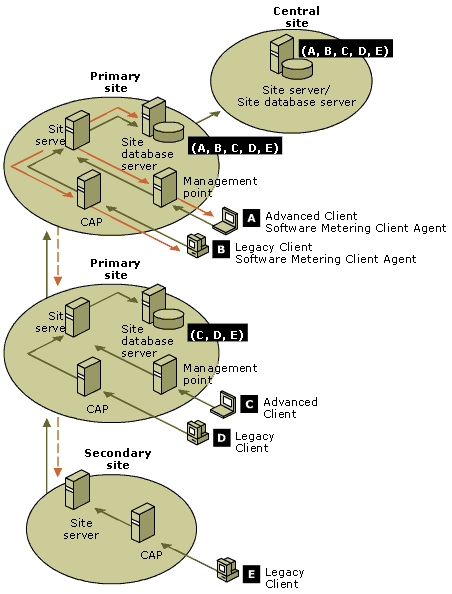


Figure 4. How the Software Metering feature in SMS 2003 captures and reports software usage information to a central site

When the Software Metering feature is enabled, SMS 2003 collects information about program activity on desktops. For more information on the Software Metering feature in SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan931z.mspx>.

### Security Patch Management

Automated patch distribution for desktops was covered in the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide. To move to the Rationalized level, you need to automate tracking of patch compliance on your organization’s desktops. SMS 2003 can track vulnerabilities and report the status of deployed updates.

For more information on security patch management using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan7lo2.mspx>.

### System Status Monitoring

System status as defined by the Infrastructure Optimization Model monitors both product compliance and desktop system status. Product compliance ensures that software complies with your organization’s guidelines. If your organization mandates that a certain version of a product is used or has guidelines to restrict certain products, product compliance will help you ensure that software installed on desktops complies with these guidelines. Your organization should also centrally monitor desktop system status. SMS 2003 can be used to monitor product compliance and generate status messages to report the activity of components on desktops.

For more information on product compliance reporting using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan7zlk.mspx>.

For more information on desktop system status reporting using 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan1bzh.mspx>.

### System Center Configuration Manager 2007

[System Center Configuration Manager 2007](http://www.microsoft.com/technet/sms/default.mspx) is the next generation systems management solution for change and configuration management for the Microsoft platform, enabling organizations to provide relevant software and updates to users quickly and cost-effectively.

System Center Configuration Manager 2007 provides the following features:

* Collecting hardware and software inventory.
* Distributing and installing software applications.
* Distributing and installing updates to software—for example, security fixes.
* Restricting computers from accessing the network if they do not meet specified requirements—for example, having certain security updates installed.
* Deploying operating systems.
* Specifying what a desired configuration would be for one or more computers and then monitoring adherence to that configuration.
* Metering software usage.
* Remotely controlling computers to provide troubleshooting support.

All of these features require that System Center Configuration Manager 2007 client software to be installed on the Windows-based computers you want to manage. System Center Configuration Manager 2007 client software can be installed on regular desktop computers, servers, portable computers such as laptops, mobile devices running Windows Mobile or Windows CE, and devices running Windows XP Embedded such as automated teller machines. Microsoft partners can write additional client software to manage computers running non-Windows operating systems.

System Center Configuration Manager 2007 sites provide a way to group clients into manageable units with similar requirements for feature sets, bandwidth, connectivity, language, and security. System Center Configuration Manager 2007 sites can match your Active Directory sites or be totally independent of them. Clients can move between sites or even be managed from remote locations such as home offices.

## Phase 4: Deploy

In the Evaluate and Plan phase, you determined the additional attributes needed to enable the Automated Tracking of Hardware and Software on Desktops requirement of the Rationalized level. In the Deploy phase, you are tasked with implementing these additional tasks and integrating them into a common process.

We will again assume that your organization has already implemented automated asset inventory (Standardized level, Patch Management), [automated desktop operating system deployment](#_Requirement:_Automated_Operating) (Rationalized level), and security patch management (Standardized level). Hence, the Deploy phase focuses on automated application deployment, software usage tracking, and system status monitoring.

For information on how to perform automated application deployment using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_51wl.mspx>.

For information on how to deploy software usage tracking using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_2019.mspx>.

For information on how to deploy product compliance reporting as part of system status monitoring using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_9u0n.mspx>.

For information on how to deploy desktop system status monitoring using SMS 2003, see <http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_4g8n.mspx>.

## Further Information

For more information on tracking hardware and software using SMS 2003, visit [Microsoft TechNet](http://www.microsoft.com/technet/sms/default.mspx) and search for “hardware and software inventory.”

To see how Microsoft deploys SMS 2003, go to <http://www.microsoft.com/technet/itshowcase/content/depsms03.mspx>.

## Checkpoint: Automated Tracking of Hardware and Software for Desktops

|  |  |
| --- | --- |
| X | Requirements |
|  | Deployed tools and procedures to automate desktop asset inventory. |
|  | Implemented procedures and technologies to automate application and operating system deployment. |
|  | Implemented tools and procedures to perform and analyze software usage tracking reporting. |
|  | Implemented best practice automated software update management. |
|  | Deployed tools and procedures to monitor desktop system status, including product compliance and system status monitoring. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Automated Tracking of Hardware and Software capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for tracking of hardware and software.

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_2).

# Requirement: Latest Two OS Versions and Service Packs on Desktops

## Audience

You should read this section if 80 percent of your desktops are not running one of the two most recent versions of the Microsoft operating system.

## Overview

In the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide, you read about the importance of limiting to two the number of different operating systems in your organization. To move from the Standardized level to the Rationalized level, your organization’s two standard operating system images need to be the most recent versions, with the latest service packs installed. The general benefits of having the two most recent operating systems in production are supportability, ease of maintenance and troubleshooting, and reduced complexity of the desktop environment. More specific benefits and tradeoffs are called out in the Evaluate and Plan phase.

## Phase 1: Assess

During the Assess phase, you need to take inventory of the desktop operating systems your organization has in production. Automating desktop asset inventory is discussed in the [Automated Tracking of Hardware and Software for Desktops](#_Asset_Inventory) requirement.

## Phase 2: Identify

In the Identify phase you will use the results of the Assess phase to determine which desktop assets should be upgraded or refreshed. At this time, you should also examine your options for upgrading users to the most current operating system or the previous version.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase will discuss the advantages and trade-offs of each operating system and examine the requirements for hardware upgrades to support your selected operating system strategy. The two latest versions of operating systems available are Microsoft Windows XP with Service Pack 2 and Windows Vista™. The following sections discuss the advantages and trade-offs of the Windows desktop operating system versions from the perspective of desktop administration and deployment.

### Windows XP and Windows Vista Advantages

Although earlier versions of Windows may still be functional for specific and limited applications within your organization, they do not contain the features that make the latest operating systems more secure, more efficient, and easier to manage. By moving your desktop computers to Windows XP or Windows Vista, you can realize the following core advantages over previous versions of Windows desktop operating systems:

**Windows XP and Windows Vista**

* Improved wireless network support
* Improved data protection and recovery
* Enhanced Web security
* Integrated firewall

**Windows Vista**

* BitLocker™ drive encryption
* Hardware abstraction layer (HAL) independence
* Language neutrality
* Improved deployment experience

#### Improved Wireless Network Support

Windows XP and Windows Vista simplify the tasks necessary for setting up a network computer and joining it to a network. Universal Plug and Play is designed to support zero-configuration, "invisible" networking, and automatic discovery for a variety of device categories from a wide range of vendors. In addition, Windows Vista supports both Internet Protocol version 4 (IPv4) and Internet Protocol version 6 (IPv6) to meet all your future networking needs.

For more information on the networking capabilities of Windows XP and Windows Vista, visit the following Web sites:

* <http://www.microsoft.com/technet/prodtechnol/winxppro/evaluate/netwkxp.mspx>
* <http://technet.microsoft.com/en-us/windowsvista/aa905087.aspx>

#### Improved Data Protection and Recovery

Windows XP and Windows Vista provide significant advancements in data recovery and protection and private key recovery. Encrypting File System (EFS), available in both operating systems, supports the use of data recovery agents (DRA) to decrypt files that have been encrypted by other users.

For more information on EFS, visit the following Web sites:

* <http://www.microsoft.com/technet/prodtechnol/winxppro/support/dataprot.mspx>
* <http://technet.microsoft.com/en-us/windowsvista/aa905073.aspx>

#### Enhanced Web Security

Security features and enhancements in Windows XP and Windows Vista provide protection to your organization’s desktops and servers that earlier versions of the Microsoft operating system did not and could not address. Implementing the latest operating systems on your desktops is the only way to ensure that you are protected against the latest attempts to breach your network. For more information on the security features of Windows XP and Windows Vista, visit the following Web sites:

* <http://www.microsoft.com/technet/security/prodtech/windowsxp/secwinxp/default.mspx#ETD>
* <http://www.microsoft.com/technet/windowsvista/security/guide.mspx>

#### Integrated Firewall

Windows XP and Windows Vista both provide an integrated firewall for desktops. Not all earlier versions of the Microsoft operating system have this capability. The *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide outlines the need for personal firewalls on desktop computers. The latest operating systems from Microsoft provide this capability integrated, so implementation and setup is easier.

For more information on personal firewalls, visit the following Web sites:

* <http://www.microsoft.com/technet/network/wf/default.mspx>
* <http://www.microsoft.com/technet/community/columns/cableguy/cg0106.mspx>

#### BitLocker Drive Encryption (Windows Vista)

BitLocker drive encryption helps protect data on a client computer. The entire Windows volume is encrypted to help prevent unauthorized users from breaking Windows file and system protections or from viewing information offline on the secured drive. Early in the startup process, BitLocker checks the client computer's system and hardware integrity. If BitLocker determines an attempt has been made to tamper with any system files or data, the client computer will not complete the startup process.

BitLocker is available in the Windows Vista Enterprise and Ultimate editions of the operating system for client computers.

For more information on BitLocker Drive Encryption, visit the following Web sites:

* <http://technet.microsoft.com/en-us/windowsvista/aa905065.aspx>
* <http://www.microsoft.com/technet/windowsvista/security/protect_sensitive_data.mspx>

#### Hardware Abstraction Layer Independence (Windows Vista)

Windows Vista introduces hardware abstraction layer (HAL) independence to make it easier to consolidate standard desktop images. For versions prior to Windows Vista, technical restrictions prevented the creation of a single image that could be deployed to all desktop hardware types. Different HALs meant you had to maintain multiple images. When managing Windows XP and Windows Vista, most organizations will need at least two or three images for the Windows XP desktops. With Windows Vista, you can consolidate your desktop images to one per hardware platform (x86 and x64). The Windows Vista operating system is also able to detect which HAL is required and automatically install it.

For more information on hardware abstraction layer independence in Windows Vista, visit the following Web sites:

* <http://technet2.microsoft.com/WindowsVista/en/library/2957d7c4-02c7-4205-afb5-f03434d8f37d1033.mspx>
* <http://www.microsoft.com/technet/technetmag/issues/2006/11/Deployment/default.aspx>

#### Language Neutrality (Windows Vista)

In Windows Vista, the entire operating system is language-neutral. One or more language packs are added to this language-neutral core to create the image that is deployed. Servicing of Windows Vista is also language-neutral, so in many cases only one security update is needed for all languages. Configuration is also language-neutral, so one unattend.xml can be used for all languages.

With Windows XP, you can either deploy localized versions of Windows XP, requiring a different image for each language, or you can deploy an English Multilanguage User Interface (MUI) version with additional language packs. There are advantages and disadvantages to each approach, but in most cases organizations that require support of multiple languages should select using the MUI option.

For more information on language neutrality in Windows Vista and to find out which versions support multiple language instances per PC, visit the following Web sites:

* <http://technet2.microsoft.com/WindowsVista/en/library/d1bc6d15-0ecc-4c12-bdae-83e41303e6f61033.mspx>
* <http://www.microsoft.com/technet/technetmag/issues/2006/11/Deployment/default.aspx>

#### Improved Deployment Experience (Windows Vista)

Windows Vista deployment tools are available for all stages of deployment, and several are integrated into a single deployment procedure using the Business Desktop Deployment (BDD 2007) Solution Accelerator, Microsoft's proven methodology and guidance on how to optimally deploy Windows Vista and the 2007 Office system. The tools available for Windows Vista deployment include the following:

* [Windows Vista Hardware Assessment](http://www.microsoft.com/technet/windowsvista/deploy/readassess.mspx). Inventory your organization’s computers across the network without the use of software agents and determine if they will be able to run Windows Vista.
* [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx). Inventory and analyze your organization's applications to ensure they work with Windows Vista.
* [Microsoft Windows User State Migration Tool (USMT)](http://lab.technet.microsoft.com/Search/redirect.aspx?title=%ee%80%80User%ee%80%81+%ee%80%80State%ee%80%81+%ee%80%80Migration%ee%80%81+%ee%80%80Tool%ee%80%81+3.0&url=http://www.microsoft.com/technet/WindowsVista/library/usmt/91f62fc4-621f-4537-b311-1307df010561.mspx). Automatically migrate the files and settings you specify from Microsoft Windows 2000 and Windows XP to Windows Vista, whether performing an in-place upgrade or migrating to a new computer.
* [ImageX](http://technet.microsoft.com/en-us/windowsvista/aa905070). Utility allows you to capture and edit Windows images.
* [Systems Management Server 2003 with Operating System Deployment Feature Pack](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/downloads/featurepacks/osdfp.mspx). Enhances SMS by providing a customizable, centralized, and scalable way to create and deploy Windows operating system images.
* [Windows System Image Manager](http://www.microsoft.com/technet/windowsvista/library/88f80cb7-d44f-47f7-a10d-e23dd53bc3fa.mspx#BKMK_TOOLS). Configure Windows Vista images by configuring components or adding/removing optional components such as languages.
* [Windows Preinstallation Environment (PE)](http://technet.microsoft.com/en-us/windowsvista/aa905120). Edit system configuration, format drives, and so on without starting the primary operating system.

For an in-depth discussion of these technologies and tools, read the “[Windows Vista Deployment Enhancements](http://technet.microsoft.com/en-us/windowsvista/aa905119)” white paper as well as the [step-by-step instructions](http://technet.microsoft.com/en-us/windowsvista/aa905079) for a basic Windows Vista install.

For more information on the Improved Deployment Experience, visit the following Web sites:

* <http://www.microsoft.com/technet/desktopdeployment/default.mspx>
* <http://technet2.microsoft.com/WindowsVista/en/library/2957d7c4-02c7-4205-afb5-f03434d8f37d1033.mspx>

### Trade-Offs

Along with all of the advantages highlighted for Windows Vista and eased deployment, there are also a few trade-offs. From the desktop administrator perspective, the primary trade-offs for Windows Vista compared to Windows XP are that deployment images are larger and system requirements increase.

#### Image Size

With Windows XP and Windows 2000, it is possible to create images that fit easily on a single CD (less than 700 MB). If your organization adds applications and drivers to that image, the size typically approaches 2–3 GB. With Windows Vista, image size begins at about 2 GB compressed. Adding applications will often expand compressed images to 4–5 GB. This will have implications on the network used to deploy Windows Vista images. Fortunately, enhancements have been made to accommodate offline deployment in case your organization’s network is not capable of deploying larger images. You can now create self-contained Lite Touch DVD or USB media to manage the deployment process offline with minimal user interaction.

#### Hardware Requirements

Windows Vista can be installed to enable two levels of user experience. The standard experience can be installed on certified Windows Vista Capable PCs, and the premium experience can be installed on Windows Vista Premium Ready PCs. The standard experience delivers the Windows Vista core attributes such as innovations in security and reliability and in organizing and finding information. Premium features may require advanced or additional hardware. The Windows Vista Premium Ready hardware can deliver premium experiences, including Windows Aero, a productive, high-performing desktop interface. The recommended tools for assessing existing collections of hardware for Windows Vista are the [Windows Vista Hardware Assessment](http://www.microsoft.com/technet/windowsvista/deploy/readassess.mspx)or [Systems Management Server 2003 with Service Pack 3](http://www.microsoft.com/technet/sms/default.mspx).

Detailed information in the following table outlines requirements of Windows Vista Capable and Premium Ready hardware.

|  |  |  |
| --- | --- | --- |
|  | ****Windows Vista Capable PC**** | ****Windows Vista Premium Ready**** |
| Processor | Modern processor (at least 800 MHz1)  CPU manufacturer information:  [Intel](http://www.intel.com/business/windowsvista/index.htm)  [AMD](http://www.amd.com/windowsvista)  [Via](http://www.via.com.tw/en/products/vista/cpu.jsp) | 1 GHz 32-bit (x86) or 64-bit (x64) processor 1 |
| System Memory | 512 MB | 1 GB |
| GPU | Microsoft DirectX® 9 Capable (WDDM driver support recommended) | Windows Aero Capable  DirectX 9-class GPU that supports:  A WDDM driver  Pixel Shader 2.0 in hardware  32 bits per pixel  Adequate graphics memory2 |
| Graphics Memory |  | 128 MB |
| HDD |  | 40 GB |
| HDD Free Space |  | >15 GB |
| Optical Drive |  | DVD-ROM Drive3 |

1Processor speed is specified as the nominal operational processor frequency for the device. Some processors have power management that allows the processor to run at a lower rate to save power.  
2Adequate graphics memory is defined as:  
  – 64 MB of graphics memory to support a single monitor at 1,310,720 or less.  
  – 128 MB of graphics memory to support a single monitor at resolutions 2,304,000 pixels or less.  
  – 256 MB of graphics memory to support a single monitor at resolutions higher than 2,304,000 pixels.  
  – Graphics memory bandwidth, as assessed by Windows Vista Upgrade Advisor, of at least 1,600 MB per second.  
3A DVD-ROM may be external (not integral, not built into the system).

### Choosing the Appropriate Mix

The result of the Evaluate and Plan phase is to determine the appropriate desktop strategy and mix of Windows XP versus Windows Vista production operating systems for your organization.

## Phase 4: Deploy

Automated deployment of operating system images is discussed in the [Automated Operating System Distribution](#_Automated_Patch_Distribution) requirement of the Core Infrastructure Optimization Model Rationalized level.

## Further Information

For more information on current desktop operating system versions, visit the following Web sites:

* <http://www.microsoft.com/technet/prodtechnol/winxppro/default.mspx>
* <http://technet.microsoft.com/en-us/windowsvista/default.aspx>

To see how Microsoft plans deployment of operating systems, go to the following Web sites:

* <http://www.microsoft.com/technet/itshowcase/content/vistaoffice.mspx>
* <http://www.microsoft.com/technet/itshowcase/content/mswxpdeploysupport.mspx>

## Checkpoint: Latest Two OS Versions and Service Packs on Desktops

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried existing production operating systems. |
|  | Determined new computer and refresh strategies in order to phase out older operating systems. |
|  | Deployed two most recent operating system versions to at least 80 percent of all desktops. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Latest Two OS Versions and Service Packs on Desktops capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practices for maintaining OS versions addressed in the [Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx) found in [BDD 2007](http://www.microsoft.com/technet/desktopdeployment/bddoverview.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_3).

# Requirement: Latest Versions of Microsoft Office on Desktops

## Audience

You should read this section if 80 percent of your desktops are not running Microsoft Office 2003 or the 2007 Microsoft Office system.

## Overview

Today, more than ever, people and organizations are using software tools to process information. These applications are being used to create materials critical to an organization’s success and therefore require careful consideration when configuring, deploying, securing, and managing them. Microsoft Office—along with supporting tools and System Center products—offers technology and guidance for IT professionals to perform these important tasks. This guide focuses primarily on the [Office Resource Kit](http://technet2.microsoft.com/Office/en-us/library/9df1c7d2-30a9-47bb-a3b2-5166b394fbf51033.mspx), underlying tools, and corresponding products to enable setup, deployment, and management of Office 2003 and the 2007 Office system.

## Phase 1: Assess

In the Assess phase, you are primarily taking an inventory of your current environment and determining which versions of Microsoft Office are present on desktops. The versions present on desktops may be different than the versions initially deployed or those maintained as part of the standard desktop image. It is recommended that you use automation to centrally inventory your environment, such as [Systems Management Server 2003](http://www.microsoft.com/technet/sms/default.mspx), the [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625), or the [Application Compatibility Toolkit (ACT)](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx).

## Phase 2: Identify

In the Identify phase you should begin determining which users should be updated. This process weighs the needs of the business and related costs and is applicable to everyone in the user environment. In the Evaluate and Plan phase, you will look at all of the deployment, security, and management features and determine the appropriate mix given your organizational needs.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, you examine the manageability features of both versions of Microsoft Office and determine from the IT perspective which users should receive each version of the software. This section will only discuss the features of each version as applicable to the IT department in your organization. For more detail on Microsoft Office usability and advantages for end users, please visit [Microsoft Office Online](http://office.microsoft.com).

The core implementer-focused considerations for Microsoft Office include:

* Planning and Architecture
* Security and Protection
* Deployment
* Operations

We will briefly discuss each of these considerations and how they are represented in the Office 2003 editions as well as the 2007 Microsoft Office system.

### Planning and Architecture

When updating to a new productivity suite, the first area for evaluation—once all computers have been inventoried—is to examine the impacts of migration and what tools are available to successfully migrate users from one suite to another. Both Microsoft Office 2003 and the 2007 Microsoft Office system offer tools and guidance to evaluate and plan for the migration.

#### Migrating to the 2007 Office System

The 2007 Microsoft Office system offers many improvements and new features in response to customer needs. Changes such as the new file format and new Setup architecture require careful planning and preparation before upgrading. Your migration planning will include evaluating the files in your environment, identifying potential conversion issues, and reviewing migration considerations for each program within the 2007 Office release.

The Office Migration Planning Manager (OMPM) enables you to examine the files in your environment and decide whether to archive them, convert them in bulk with the Office File Converter available in OMPM, or convert them manually. You will also determine the approach to upgrade and migration within your organization.

Planning a migration to 2007 Office release includes the following:

* **Review top migration issues.** For more information, see [Review migration issues for the 2007 Office system](http://technet2.microsoft.com/Office/en-us/library/377a9113-b8bb-498c-a846-26759c5dac151033.mspx).
* **Review differences between 2007 Office release and Office 2003.** For more information, see [Differences between the 2007 Office system and Office 2003](http://technet2.microsoft.com/Office/en-us/library/a9189734-e303-4d7d-93eb-3584c358d1c91033.mspx). Many of these issues are detected by the OMPM Office File Scanner. Others might require a difference in user behavior, or they might require changes in custom solutions.
* **Review file format changes.** For quick information about file format changes, see [FAQ: File format](http://technet2.microsoft.com/Office/en-us/library/94bce792-e361-453b-b144-883e2aa20a2e1033.mspx). For more in-depth information about the new file formats, see [File format reference](http://technet2.microsoft.com/Office/en-us/library/cce79538-711f-4686-9a31-2bdc7dd999d51033.mspx).
* **Review collaboration issues for 2007 Office release.** For more information, see [Collaborating with previous versions of Office and other programs](http://technet2.microsoft.com/Office/en-us/library/c6189fcd-3668-4cd7-8bac-5c37e338bde21033.mspx).
* **Assess your environment with OMPM.** This involves the following steps:
* [Install and configure OMPM File Scanner](http://technet2.microsoft.com/Office/en-us/library/1850987f-87bb-47e9-b370-f4b8af3c39d71033.mspx)
* [Distribute OMPM File Scanner](http://technet2.microsoft.com/Office/en-us/library/1e60de90-e9f4-421a-a432-46d44799cfd41033.mspx)
* [Prepare a SQL database for OMPM](http://technet2.microsoft.com/Office/en-us/library/2a95c83f-8a2f-4da0-a8b6-3d7ae0d21e511033.mspx)
* [Import OMPM log files into the database](http://technet2.microsoft.com/Office/en-us/library/eabaaa29-afc9-4cb3-bdd0-2f09d3fae1831033.mspx)
* [Analyze reports from OMPM](http://technet2.microsoft.com/Office/en-us/library/be467931-7aa8-4bc4-b4e1-9273eca328231033.mspx)

#### Migrating to Office 2003

Migrating users and files from Office 97, Office 2000, and Office XP to Office 2003 is a relatively straightforward process. These versions of Microsoft Office share many common file formats and a common version of the [Office Converter Pack](http://office.microsoft.com/en-us/ork2003/HA011513581033.aspx), which can be found on the Office 2003 Resource Kit [Office 2003 Resource Kit Downloads](http://office.microsoft.com/search/redir.aspx?AssetID=XT011513161033&CTT=5&Origin=1033) page.

The Office Converter Pack bundles together a collection of file converters and filters that can be deployed to users. The Converter Pack can be useful to organizations that use Microsoft Office 2003 in a mixed environment with earlier versions of Office and other applications, including Office for the Macintosh and third-party productivity applications. Although these converters and filters have been available previously, they are packaged together here for convenient deployment.

For details about how to install and use the Office Converter Pack, visit the [Office 2003 Resource Kit Toolbox: Office Converter Pack](http://office.microsoft.com/en-us/ork2003/HA011513581033.aspx) Web site.

### Security and Protection

The security and protection of files is becoming increasingly scrutinized by organizational policies and government regulations. The 2007 Office system addresses this by offering new functionality aligned with Group Policy and improved setup using the new Office Customization Tool. Office 2003 also added functionality over legacy versions with improvements in file encryption, macro security, ActiveX controls, and Trusted Publisher management.

#### Security in the 2007 Office System

The 2007 Microsoft Office system has many new security settings that can help you mitigate threats to your organization's resources and processes. In addition, the 2007 Office release has many new privacy options that help you mitigate threats to users' private and personal information. Determining which new settings and options are appropriate for your organization can be a complex task involving numerous critical planning decisions. To help you minimize the time spent planning settings and options, use the four-step security planning process described in this guide. This systematic decision-making approach is designed to help you choose settings and options that maximize protection and productivity in your organization.

The new Office Customization Tool (OCT) replaces the Custom Installation Wizard and is the main deployment tool for configuring and managing security settings. Additionally, Administrative Templates (.adm files) can be loaded directly into the Group Policy Object Editor and applied to client computers as local policies or domain-based policies.

The [Office Resource Kit](http://technet2.microsoft.com/Office/en-us/library/6642d67f-9418-459c-8235-b308b09b735b1033.mspx) outlines a four-step approach to securing the 2007 Office system:

1. Determine which tools you need in order to deploy security settings and privacy options in your organization.
2. Identify the threats that pose a risk to your organization.
3. Evaluate the default settings and options that mitigate those threats.
4. Determine which additional settings and options you need to deploy to minimize risks to your organization's resources and processes.

The following process diagram depicts these steps.

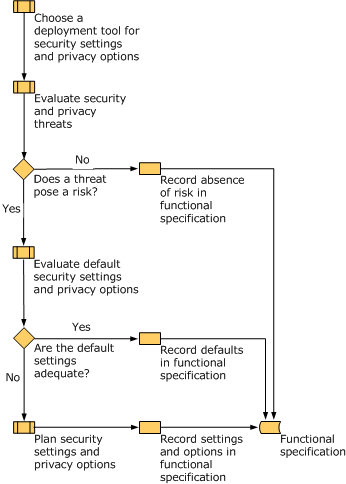


Figure 5. The four-step approach to securing the 2007 Office system

For more detail on these steps, visit the [Office Resource Kit Security and Protection](http://technet2.microsoft.com/Office/en-us/library/6642d67f-9418-459c-8235-b308b09b735b1033.mspx) guidance on Microsoft TechNet.

#### Security in Office 2003

To help address growing concern about the security of information and systems, several new features were included in Office 2003 for administrators and users. Some of the new improvements are described in the following sections.

##### Revised Macro Security

Although the legacy macro security methods helped to address many security-related issues, a few subtle improvements have been made to how documents, attachments, and linked references are opened. For more information on the effects of these improvements on users, as well as how the administrator can configure security settings in the Custom Installation Wizard, see [Macro Security Levels in Office 2003](http://office.microsoft.com/search/redir.aspx?AssetID=HA011403071033&CTT=5&Origin=HA011403021033).

##### Revised Trusted Publishers Store Management

When administrators accept certificate of trusts from external vendors, they can now more easily roll out those certificates to others by using Active Directory. It is also possible to remove an installed and trusted certificate of trust if you no longer require it or suspect it was compromised.

For more information on managing the Trusted Publishers store, see [Working with Trusted Trust Publishers](http://office.microsoft.com/search/redir.aspx?AssetID=HA011403091033&CTT=5&Origin=HA011403021033).

##### Revised Microsoft ActiveX® Controls

The concern about how ActiveX controls the Start and Run buttons on users' computers is more important than ever. Office 2003 administrators have more control to defend against unknown or ill-defined controls that may possess security flaws. This allows you to set the degree of risk you are willing to accept from an unknown ActiveX control when it starts. For more information on ActiveX controls as they relate to security, see [ActiveX Controls and Office Security](http://office.microsoft.com/search/redir.aspx?AssetID=HA011403101033&CTT=5&Origin=HA011403021033).

##### New Encryption Types

Office 2003 added new encryption types and the ability to set all Office applications to use a specific encryption type as its default. This does not mean that every document will have encryption when it is saved; it only means that if a password is set to encrypt the document, the user does not have to select an encryption type to use. For more information on configuring Office 2003 for encryption, see [Important Aspects of Password and Encryption Protection](http://office.microsoft.com/search/redir.aspx?AssetID=HA011403111033&CTT=5&Origin=HA011403021033).

##### Revised Core Office Programming Objects

Due to the security review of all Office applications, the core objects were updated to help eliminate the classic buffer overflow attack to any data entry points. Improvements were also made to handling user IDs and passwords stored within code. For more information on Office code objects as related to security, see [Important Aspects of Password and Encryption Protection](http://office.microsoft.com/search/redir.aspx?AssetID=HA011403111033&CTT=5&Origin=HA011403021033).

### Determining the Appropriate Office Versions for Your Users

This guide highlights the configuration, security, and deployment considerations for Office 2003 and the 2007 Office system. Determining the appropriate version distribution strategy for your users will be consistent with any new software acquisition and should take into account the benefits and trade-offs for end users, file security and protection, file version compatibility, license costs, deployment costs, and operations costs. The result of this exercise will enable you to determine your organization’s strategy for managing a single Office version or multiple Office versions and determine which users will receive upgrades.

## Phase 4: Deploy

The overall deployment methodologies for Office 2003 and the 2007 Office system are for the most part consistent with each other. The tools used to automate software distribution and installation of Microsoft Office are the same as those called out in the requirement for [Automated Tracking of Hardware and Software for Desktops](#_Requirement:_Automated_Tracking) for the Core Infrastructure Optimization Rationalized level. The Rationalized level in Core Infrastructure Optimization requires that the organization has fully automated software and operating system distribution using such technologies as [Systems Management Server 2003](http://www.microsoft.com/technet/sms/2003/library/deployoffice2003_sms2003.mspx).

Office installations can occur as stand-alone application installations using technologies such as [Systems Management Server 2003](http://www.microsoft.com/technet/sms/2003/library/deployoffice2003_sms2003.mspx) (or, in limited cases, Group Policy) or at the time of desktop image deployment. All three methods require careful attention during the planning and configuration phases.

[Business Desktop Deployment 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/OfficeDep_4.mspx) guidance generally treats Office installations as part of the core desktop image. Based on the image strategy in your organization, this can mean that the Office package is integrated as a component of the core image itself in a thick image strategy, or it can be installed after a thin operating system image is present on the targeted machine. In the instance of thin image strategy, the Office deployment task is essentially the same as installing Office on a legacy system, with a notable exception being the uninstall of the legacy Office version.

#### Deploying the 2007 Office System

Whether part of a desktop image deployment or as a stand-alone application deployment, the 2007 Office system deployment process should follow specific milestones and objectives. For more detailed guidance, visit the [Business Desktop Deployment 2007 Office Deployment Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/OfficeDep_4.mspx). The key milestones and objectives are depicted in the following diagram and listed below.

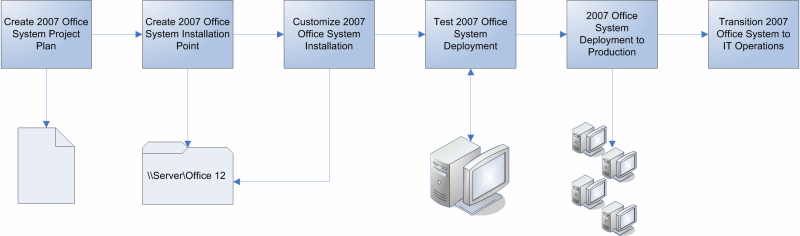


Figure 6. Key milestones and objectives of the 2007 Office system deployment

* **Creating a project plan**. As with any project, careful planning leads to greater chances of success. In this phase, the team analyzes current Microsoft Office deployments, plans migration of documents and settings, determines optimal placement of deployment servers, and acquires resources for completing the project.
* **Creating an installation point**. The first phase of development, creation of the 2007 Office system installation point, creates a shared source location containing the 2007 Office release installation files.
* **Customizing installation**. Most organizations require some changes to the default settings for the 2007 Office release. Consolidate these settings into a Microsoft Office customization file that can then be applied to the installation point.
* **Testing Microsoft Office deployment**. Before releasing the 2007 Office system to production, careful testing of the 2007 Office system deployment process ensures that the deployment occurs as planned.
* **Deploying to production**. Activating deployment procedures to provide the 2007 Office release to client computers.
* **Transitioning to IT Operations**. After the deployment plan has been executed, the deployment infrastructure is handed off to IT Operations for long-term operation and management.

For more guidance on 2007 Office system deployment, visit the [Desktop Deployment Center on Microsoft TechNet](http://www.microsoft.com/technet/desktopdeployment/default.mspx) and read the [Office Deployment Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/OfficeDep_4.mspx).

#### Deploying Office 2003

The Office 2003 deployment will follow the same general milestones and guidelines as the 2007 Office System. The tools used to customize the installation are different than with the 2007 release and provide a fair amount of flexibility for customizing the installation to your organization’s needs.

Detailed guidance for [Deploying Office 2003 Using Systems Management Server 2003](http://www.microsoft.com/technet/sms/2003/library/deployoffice2003_sms2003_3.mspx) is available on Microsoft TechNet. If you are not managing application installations using SMS 2003, you can also use Group Policy to deploy Office 2003 to client computers. Using Group Policy software installation features, you can assign or publish Office 2003 to all the users or computers in a designated group.

For large or complex organizations, Systems Management Server 2003 offers more sophisticated functionality, including inventory, scheduling, and reporting features. However, using Group Policy to deploy Office 2003 can be a good choice in the following settings:

* Small- or medium-sized organizations that have already deployed and configured the Active Directory directory service.
* Organizations or departments that comprise a single geographic area.
* Organizations with consistent hardware and software configurations on both clients and servers.

For detailed guidance about deploying Office 2003 Editions by using Group Policy, see <http://office.microsoft.com/en-us/ork2003/HA011402011033.aspx>.

## Operations

Operations management for Microsoft Office is consistent with recommendations defined in the [Automated Tracking of Hardware and Software for Desktops](#_Requirement:_Automated_Tracking) requirement at the Rationalized level in the Core Infrastructure Optimization Model. Operations specific to Office 2003 and the 2007 Office system for applying software updates (patches) and enforcing Group Policy configuration standards are highlighted below.

### Updating Office (Office 2003 and the 2007 Office System)

Your organization should follow the desktop patch management guidelines discussed in the *Core IO Implementer Resource Guide: Basic to Standardized*. Verified updates are distributed directly to the client to ensure that existing Office installations have the latest software updates.

### Enforcing Group Policy Settings (2007 Office System)

In a Microsoft Windows-based network, administrators can use Group Policy settings to help control how users work with the 2007 Microsoft Office system. Administrators can use Group Policy settings to define and maintain an Office configuration on users' computers. Unlike other customizations—for example, default settings distributed in a Setup customization file—policy settings are enforced and can be used to create highly managed or lightly managed configurations.

You can use the 2007 Office release policy settings to:

* Control entry points to the Internet from the 2007 Office release applications.
* Manage security settings in the 2007 Office release applications.
* Hide settings and options that are unnecessary for users to perform their jobs and that might distract users or result in unnecessary calls for support.
* Create a highly managed standard configuration on users' computers.

You can set policy settings that apply to the local computer and every user of that computer, or that apply only to individual users. Per-computer policy settings are set under the **Computer Configuration** node of the Group Policy Object Editor Microsoft Management Console (MMC) snap-in and are applied the first time any user logs on to the network from that computer. Per-user policy settings are set under the **User Configuration** node and are applied when the specified user logs on to the network from any computer. Group Policy is also applied periodically in the background after it is initially processed at startup and logon.

For detailed information about the Group Policy infrastructure, see [Group Policy Technical Reference](http://go.microsoft.com/fwlink/?LinkId=80200) on the Microsoft TechNet site.

## Further Information

For more technical information on Microsoft Office, go to the [Microsoft Office System TechCenter](http://www.microsoft.com/technet/prodtechnol/office/default.mspx) on TechNet.

To learn how Microsoft deployed Office Professional Edition 2003 to desktops, go to <http://www.microsoft.com/technet/itshowcase/content/deskdeployoffice2003.mspx>.

## Checkpoint: Latest Versions of Microsoft Office on Desktops

|  |  |
| --- | --- |
| X | Requirements |
|  | Evaluated the latest versions of Office and defined plan to consolidate Office versions on production workstations. |
|  | Deployed latest versions of Office to desktops. |
|  | Defined plan for managing Office configurations. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Latest Versions of Microsoft Office on Desktops capabilities of the Infrastructure Optimization Model.

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_4).

# Requirement: Compatibility Testing and Certification of Software Distributions

## Audience

You should read this section if you do not test and certify application compatibility on 80 percent of new or updated applications before deploying them to your desktops.

## Overview

In general, applications are highly optimized for a specific operating system or operating system version. Application compatibility problems can arise when you have applications that were designed to run under earlier versions of Microsoft Windows operating systems. The rationale for testing applications is to ensure that deployment of any new software component does not affect end-user productivity or result in downtime. Compatibility testing is also mentioned as a required process for patch management and operating system deployment in the Core Infrastructure Optimization Model.

Even with these advanced compatibility features included in Microsoft products, you need to ensure that all your applications function properly under the latest Microsoft Windows operating systems before you distribute those applications to your organization’s desktops. This guidance is based on the [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) and the [Application Compatibility Feature Team Guide in Business Desktop Deployment 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppCompact_1b.mspx), both free resources from Microsoft that assist in identifying and managing your overall application compatibility management.

## Phases 1: Assess

The Assess phase is important for the deployment process whether you are deploying new operating systems and intend to overlay applications as part of the deployment, deploying the applications themselves to existing machines, or deploying updates to applications. In the Assess phase, your organization should gather an inventory of the applications and data components in the environment that affect application compatibility. These items include:

* Operating system version
* Service-pack level
* Geographic location
* Computer manufacturer model and type
* Applications installed
* Business unit in which the computer is used
* Organizational role that the user perform

### Inventory and Collect Data

The [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) provides a way to gather inventory data through the use of distributed compatibility evaluators and the developer and tester tools. Data can be collected for operating system changes of various magnitude, from large events (such as an operating system upgrade), to medium events (such as a browser upgrade), to smaller events (such as a Windows Update release). Having the ability to collect compatibility data into a single centralized store has significant advantages in reducing organizational risk during platform changes. As a component of the Application Compatibility Toolkit, the Inventory Collector examines your organization's computers to identify the installed applications and system information.

[Systems Management Server (SMS) 2003 Software Inventory](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_0f3b.mspx) can also be used to inventory or audit software installed on computers within the organization. Typically, you would use SMS 2003 to identify applications with known compatibility issues. However, it is possible to create scripts or other executables to perform customized application compatibility inventorying, and then use the SMS Software Inventory to report the results to SMS.

## Phase 2: Identify

In the Identify phase, you collect the proposed applications or operating systems to be tested and validated. For example, if you are deploying the 2007 Office system, your organization will identify the edition and selected applications to be tested in a pre-production environment. You will also ensure that all targeted operating systems or dependent applications are present in your pre-production test environment.

If your organization does not currently have a test environment that emulates the production environment, the Identify phase will also include building the test environment. This environment can be built using an adequate sample of physical machines with appropriate hardware and software components installed; however, it is generally recommended that the environment incorporate the use of virtualization technologies. For guidance on building a virtual test environment, please see [Windows Server System Reference Architecture Virtual Environments for Development and Test (WSSRA-VE)](http://www.microsoft.com/technet/solutionaccelerators/wssra/ve/default.mspx).

## Phase 3: Evaluate and Plan

Once you have inventoried your environment, identified all of the applications to be deployed, and built a test environment, you can begin evaluating your applications, certifying them, and planning for deployment. The [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) includes several components to evaluate compatibility.

### Common Compatibility Problems

There are several reasons why an application written specifically for a different version of Windows—especially the Microsoft Windows 2000 Professional, Windows Me, Windows NT® Workstation 4.0, Windows 98, and Windows 95 operating systems—may manifest problems when run under Windows XP or Windows Vista. Most problems fall into the following categories:

* Setup and installation
* Kernel-mode drivers
* Permissions
* Heap management
* Firewall
* Distributed Component Object Model (DCOM)
* Internet Explorer

For detailed information about common compatibility problems, see the following:

* **Windows XP:** <http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/appcom/default.mspx>
* **Windows Vista:** <http://www.microsoft.com/technet/windowsvista/appcompat/entguid.mspx>

### Compatibility Evaluators

The Application Compatibility Toolkit and Application Compatibility Toolkit Data Collector (ACT-DC) use compatibility evaluators to collect and process your application information. Each evaluator, described in the following list, performs a set of functions, providing a specific type of information to ACT:

* **User Account Control Compatibility Evaluator (UACCE).** Enables you to identify potential compatibility issues that are due to permission restrictions enforced by the User Account Control (UAC), formerly known as Limited User Accounts (LUA). Through compatibility logging, UACCE provides information about potential application permission issues and ways to fix the problems so that you can deploy a new operating system.
* **Update Compatibility Evaluator (UCE).** Provides insight and guidance about the potential effects of a Windows operating system security update on your installed applications. The UCE dynamically gathers application dependencies and is deployable to both your servers and client computers in either a production or test environment. The compatibility evaluator collects information about the modules loaded, the files opened, and the registry entries accessed by the applications currently running on the computers and writes that information to XML files uploaded to the ACT database.
* **Internet Explorer Compatibility Evaluator (IECE).** Enables you to identify potential Web application and Web site issues that occur due to the release of a new operating system. IECE works by enabling compatibility logging in Internet Explorer, parsing logged issues, and creating a log file for uploading to the ACT Log Processing Service.
* **Windows Vista Compatibility Evaluator.** Enables you to identify issues that relate to the Graphical Identification and Authentication (GINA) DLLs, to services running in Session 0 in a production environment, and to any application components deprecated in the Windows Vista operating system.

### Test Plan

It is important to approach testing and certifying applications systematically. Develop a test plan in which you will exercise all the features of an application that your organization is likely to use. To simplify discovering potential conflicts between applications and the operating system, you can include Microsoft application compatibility technologies as a key part of your test plan. The Application Compatibility Toolkit provides tools for developers to test setup packages, Web sites and Web applications with Internet Explorer 7, and applications.

### Compatibility Analysis and Mitigation

After collecting your compatibility data, you then analyze your findings and begin to plan for application compatibility mitigation, if needed. The Application Compatibility Toolkit also provides features and tools to help you organize, rationalize, and prioritize the data. The result of Compatibility Analysis should be to determine whether the applications are compatible on the user machines targeted for software distribution and, if necessary, which fixes need to be made to make them compatible.

The key deliverables from the analysis and mitigation processes are application mitigation packages for the deployment. You can create these packages automatically by using application compatibility tools, such as ACT. For other application mitigation methods, you can create the packages and the installation scripts or executables (including .msi files) manually.

The Application Compatibility Manager from ACT packages the solutions for deployment in the test and production environments. The Solution Builder contains a component called the Packager, which can take as input any number of Analyzer files or Compatibility Administrator files and create a self-extracting executable package.

It is often necessary to manually create the packages to be installed. In some instances, this process may include creating scripts or .msi files to facilitate installation.

See the [Application Compatibility Feature Team Guide in Business Desktop Deployment 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/AppCompact_6.mspx) requirement for more information.

### Application Certification

After all applications are tested and mitigation strategies are in place, you can record it as certified in your test results. Any compatibility issues that you discover during testing must be well documented and reported to stakeholders and those responsible for application release in your organization.

## Phase 4: Deploy

The Deploy phase discusses the deployment of mitigation packages alone. For information about application deployment and recommended tools, see the requirement for [Automated Tracking of Hardware and Software for Desktops](#_Automated_Tracking_of) at the Rationalized level in the Core Infrastructure Optimization Model.

You can deploy the application mitigation packages much like deploying software updates, by using automated software distribution such as:

* [**SMS 2003**](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/cpdg/plan47zc.mspx)*.* Use the software distribution feature in SMS 2003 to deploy the mitigation packages when the organization has an existing SMS 2003 infrastructure.
* [**Group Policy Software Installation**](http://technet2.microsoft.com/WindowsServer/en/library/b238ecdb-cda5-402b-9b3d-f232045a30fa1033.mspx). Use the Group Policy Software Installation feature in Active Directory to deploy the mitigation packages when the organization has an existing Active Directory infrastructure.

For each method, create an installation package (such as an .msi file) to automate the installation of the mitigation package. Use the defined application deployment process for your organization to deploy the installation packages.

## Further Information

For more information on application testing, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “application compatibility.”

To see how Microsoft does application compatibility testing, go to <http://www.microsoft.com/technet/itshowcase/content/appcompattcs.mspx>.

## Checkpoint: Compatibility Testing and Certification of Software Distribution

|  |  |
| --- | --- |
| X | Requirements |
|  | Collected and analyzed the application inventory in your organization to build your application portfolio. |
|  | Implemented standard testing of your mitigation strategies to create your application mitigation packages. |
|  | Implemented standard processes to resolve any outstanding compatibility issues to report compatibility mitigation to management. |
|  | Implemented automated deployment of all compatibility mitigation packages. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Compatibility Testing and Certification of Software Distributions capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for software certification and testing so that applications are maintained to a known standard.

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_5).

# Requirement: Patch Management for Servers

## Audience

You should read this section if you do not have a patch management solution for 80 percent of your servers.

## Overview

In the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide, *you* read about patch management and distribution to desktops. To move from the Standardized level to the Rationalized level, you need to extend patch management to your servers. The tools and procedures for updating Windows-based servers are common with those used to update Windows-based desktops.

Although many of the processes are shared, there are several notable exceptions when patching servers and dependencies on other requirements in the Core Infrastructure Optimization Model. Servers often provide mission-critical functions with service level agreements (SLAs), depending on the server’s availability. Minimizing unplanned server downtime is a key operational and server patch management requirement because, unlike desktop downtime, server downtime can often impede an entire IT service or sometimes the entire organization from running. The Rationalized level begins to introduce SLAs, which often stipulate allowable maintenance intervals, especially when maintaining servers.

Patch management guidance in the Core Infrastructure Optimization Model is based on [Patch Management Solution Accelerator content](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/default.mspx). Specific guidance is available for patch management using Systems Management Server (SMS) 2003, SMS 2.0, and Software Update Services (SUS) 1.0. The core concepts in these guides also apply to Windows Server Update Services (WSUS) and System Center products. For the latest information on patch management, visit the [Update Management Solution Center on Microsoft TechNet](http://www.microsoft.com/technet/updatemanagement/default.mspx).

As with desktop patch management, the phases of Assess, Identify, Evaluate and Plan, and Deploy and corresponding deliverables of each phase are identical to those described in the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide as a requirement for the Standardized level in the Core Infrastructure Optimization Model.

## Further Information

For more detailed information on patch management, see the “Automated Patch Distribution” section in *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized*. You can also visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “patch management.”

To see how Microsoft addresses patch management, go to <http://www.microsoft.com/technet/itshowcase/content/sms03spm.mspx>.

## Checkpoint: Patch Management for Servers

|  |  |
| --- | --- |
| X | Requirements |
|  | Implemented process and tools to inventory hardware and software assets. |
|  | Implemented process and tools to scan client computers for software updates. |
|  | Established a process to automatically identify available patches. |
|  | Established standard testing for every patch. |
|  | Implemented patch distribution software. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Patch Management for Servers in the Infrastructure Optimization Model. We recommend that you follow additional best practices for patch management addressed in the [Patch Management Solution Accelerator for SMS 2003](http://www.microsoft.com/downloads/details.aspx?FamilyId=E9EAB1BD-13E7-4E25-85C5-CE2D191C3D63&displaylang=en).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_6).

# Requirement: Guaranteed Secure Communications with Mobile Devices

## Audience

You should read this section if you do not have a secured and guaranteed way to verify secure communications between your corporate network and mobile devices.

## Overview

As organizations consider mobile enterprise solutions, a key evaluation point is security. Mobile communication solutions need to be safe and reliable, whether they involve personal information or confidential transactions in the workplace. Personal digital assistants (PDAs) and smart phones are as important as laptop PCs when it comes to an organization's security plan.

In *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized,* you read about establishing security policies as part of your overall management of mobile devices. To move to the Rationalized level, you need to automate enforcement of those security policies, especially in the area of remote communications. When you have put passwords and data encryption in place, you have taken the first steps to secure communications between your corporate network and mobile devices.

## Phase 1: Assess

As discussed in the Basic to Standardized guide, during the Assess phase it is important to take an inventory of the mobile devices connected to your infrastructure and how people are currently using mobile devices. Organizations need to track and manage several areas of mobile-device use.

## Phase 2: Identify

In the Identify phase, your organization needs to determine an appropriate mobile-device security level. Depending on your business and data security needs, end users may connect to your network with loosely controlled personal devices or with managed, company-provided devices. The next steps primarily focus on mobile-device authentication and how to deploy that capability in your organization.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, your organization should consider which tools or technologies can be used to guarantee secured communications with your mobile users. There are many mechanisms and solutions available to help administrators take the next step in guaranteeing secure mobile communications. Windows Mobile 5.0 and Windows Mobile 6.0 can be combined with Microsoft Systems Management Server (SMS) 2003 to provide a centralized mobile device provisioning, management, and policy enforcement solution. In addition, numerous third-party software providers offer systems management solutions. Using these solutions, a centralized IT organization can maintain an asset inventory of the devices that connect to the corporate network and can automatically fix configuration settings and distribute software updates as they become available. For a sample list of systems management solutions for Windows Mobile-powered devices, please visit the [Windows Mobile Solutions Provider](http://www.microsoft.com/windowsmobile/business/solutions/default.mspx) Web site and search the Software Solutions section under the Systems Management category. The IT Management category in the Vertical Market Solutions section might also provide valuable information.

The next step in securing information on a handheld device is to protect the device against unauthorized access.

### Authentication

Various mechanisms are available to identify and authenticate users. Windows Mobile certificate authentication was developed to help mitigate security risks on your mobile device. Current versions of Windows Mobile software support X.509 certificates, which provide a means for authenticating applications, users, operators, and servers. The certificates may be protected, stored, managed, and deleted on the mobile device.

To achieve a higher level of protection, Microsoft recommends that you use two of the following three approaches (often referred to as two-factor authentication):

* Something the user knows (for example, a password).
* Something the user has (for example, a security certificate in a smartcard or a SecurID token).
* Something that is part of the user (for example, a fingerprint).

In certain cases, additional authentication may be required. These include:

* Applications that require user authentication before they will run. This requirement may apply if the application hasn’t been used for a certain length of time, or it may occur on a repeating basis (for example, every 15 minutes).
* A data storage card that has its own authentication mechanism to decrypt its data.
* Additional authentication for accessing an organization’s private network. For example, Exchange Server 2003 and Exchange Server 2007 use Active Directory authentication to provide access to corporate e-mail, calendar, and contacts from mobile devices. With Exchange Server 2003 Service Pack 2 (SP2) and newer, devices can use a digital certificate for authentication so that users do not need to provide their network credentials. This reduces the risk that users’ credentials will be compromised.
* An additional logon step for accessing a protected shared file server.
* Additional sign-on credentials to access certain Web sites.

Other protections against unauthorized access to the devices available in Windows Mobile software include several forms of physical device security technology:

* **Power-on passwords.** Current versions of Windows Mobile devices support power-on passwords to help protect access to the device. Windows Mobile Pocket PC also supports strong alphanumeric power-on passwords—that is, passwords requiring at least seven characters, including a combination of uppercase and lowercase letters, numerals, and punctuation. A four-digit password can also be associated with the phone card (Subscriber Identity Module, or SIM) for GSM devices. For greater protection, all passwords are hashed (converted into a different form, making them harder to break) before being stored. When a user attempts to access the device with an incorrect password, the system imposes a time delay before allowing access again—a delay that increases exponentially with each attempt. In addition, Pocket PC File Explorer software requires user authentication for accessing shared Windows-based file servers. For further protection, an organization can set up automatic enforcement of its authentication policies using centralized management software.
* **Cabinet (.cab) file signing.** This uses third-party software to digitally sign a file using an X.509 digital certificate. This provides a way to determine the origin of the file and whether the file has been altered after it was signed.
* **Device management security technology.** This enables over-the-air changes to be made in a way that helps protect against hackers. Most Windows Mobile devices that include wireless data functionality include some degree of device management security to help prevent arbitrary applications from being downloaded and executed over the air.
* **Application-level security**. For such applications as Microsoft Internet Explorer Mobile, ActiveSync®, e-mail attachments, and infrared beaming. This type of security can use any of a number of approaches, ranging from requiring users to enter their passwords in order to gain access to applications, to authentication mechanisms such as biometrics or smart cards. The requirement could be set up to apply to each access attempt, to apply only when the application hasn't been used within a certain time period, or to require reauthorization at periodic intervals.

## Phase 4: Deploy

Once your organization has determined the appropriate security controls and mechanisms to deliver and enforce the selected security strategy, the Deploy phase includes all of the processes to implement and maintain your security strategy.

## Further Information

For more information on authentication and digital certificates for mobile devices, go to the following Web sites:

* <http://blogs.msdn.com/windowsmobile/archive/2005/12/17/security_model_faq.aspx>.
* <http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfp_3.mspx>.

To see how Microsoft addresses secure mobile communications, go to <http://www.microsoft.com/technet/itshowcase/content/trustmes.mspx>.

## Checkpoint: Guaranteed Secure Communications with Mobile Devices

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried mobile devices connecting to your network. |
|  | Determined a communication security strategy appropriate for your needs. |
|  | Implemented mobile device authentication to all connected devices. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for the Guaranteed Secure Communications with Mobile Devices requirement of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practices for secure communications with mobile devices addressed in the [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_7).

# Requirement: Access to Web Applications Using WAP or HTTP for Mobile Devices

## Overview

The integration of mobile devices, the Internet, and wireless connectivity provides an exciting opportunity for organizations to extend the reach of their information and services to mobile professionals. The potential results include improved productivity, reduced operational costs, and increased customer satisfaction. The ability to access the Internet and Internet application from mobile devices is the key to this increase in productivity.

## Phase 1: Assess

During the Assess phase, you are looking for mobile devices in your organization and the Web applications in your organization accessible via the Internet. The Web applications referred to in this level of the model are limited to those accessible via the secured or unsecured Internet access and not LOB applications specific to your organization’s Intranet.

## Phase 2: Identify

In the Identify phase, you begin to look at the Web applications that would potentially benefit end-user productivity and at the devices discovered in the Assess phase. You will also identify the devices capable of supporting HTTP or WAP browsing as well as meet the requirements you previously defined for secured communication.

## Phase 3: Evaluate and Plan

During the Evaluate and Plan phase, the goal is to determine which Web applications can be currently used with mobile device browsers, the usability of these applications per device, which devices perform the best when accessing these applications, and finally which investments should be made to either tailor Web applications to mobile devices or standardize mobile device hardware.

### Standardizing Devices

As the use of mobile devices increases in your organization, the need to control types of mobile devices also increases. Without standardization, the mix of mobile devices connecting to your corporate network would be nearly impossible to manage. User authentication, standardization of operating systems, patch management, and other everyday administrative controls can only be effectively managed when you have established an organizational standard for each type of mobile device. For more information on managing mobile devices, go to <http://www.microsoft.com/technet/solutionaccelerators/mobile/evaluate/mblmange.mspx>.

You need to consider many issues and device features when planning a mobile device solution for your organization. For guidance in planning a mobile device solution, go to <http://www.microsoft.com/technet/archive/itsolutions/mobile/deploy/mblwirel.mspx?mfr=true>.

There are several operating systems available for mobile devices. [Windows Mobile](http://www.microsoft.com/windowsmobile/articles/benefits.mspx) devices offer access to Web-based applications with extensive security and authentication features. For additional information on deploying, maintaining, and supporting Windows Mobile devices, visit <http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx>.

### Internet Access

There are numerous reasons for mobile devices to have the ability to access the Internet. Among these are:

* Software upgrades and patches.
* Corporate data access and synchronization.
* Access to Web-based applications.

This section of the guide addresses access to Web-based applications through Hypertext Transfer Protocol (HTTP) and Web Access Protocol (WAP).

### WAP

WAP is a communications protocol that can be thought of as being similar to the combination of HTTP and HTML, but optimized to account for the low memory, low bandwidth, and limited resolution of mobile devices. For more information on WAP, go to <http://www.wirelessdevnet.com/channels/wap/training/wapoverview.html>.

### Web-based Applications

Employees who use mobile devices in their day-to-day job functions often need access to information most readily available on the Internet. This information is usually dynamic (time-sensitive or constantly changing), or it is retrievable based on search criteria. Examples of applications that present this type of information are stock quotes and transactions, e-mail, sports scores, real estate listing services, and map services.

These services can be accessed through a mobile device if that device has a WAP-designed browser that simplifies the content to account for the restrictions of mobile devices. For more information on developing applications for mobile devices, read about [Microsoft ASP.NET mobile controls](http://msdn2.microsoft.com/en-gb/library/aa286514.aspx) on MSDN.

## Phase 4: Deploy

Once your organization has determined the appropriate plan for providing Web application access to mobile device users, the Deploy phase includes all of the processes to implement and maintain your plans.

## Further Information

For more information on mobile devices, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “mobile device” or “WAP.”

## Checkpoint: Access to Web Applications Using WAP or HTTP for Mobile Devices

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried mobile devices connecting to your network and Web applications currently consumed or potentially consumed by mobile device users. |
|  | Developed and implemented a strategy to optimize Web applications for mobile device users, update mobile device hardware, or both. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Access to Web Applications using WAP or HTTP for Mobile Devices requirement of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practices for secure communications with mobile devices addressed by the [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_8).

# Requirement: Server Consolidation and Virtualization

## Audience

You should read this section if you do not have a plan for server consolidation with virtualization.

## Overview

Consolidation of physical infrastructure, in general, is an effective business strategy. Consolidation of locally situated physical servers has proven effective in reducing server sprawl and, thereby, improving IT efficiency, enhancing flexibility, and reducing Total Cost of Ownership (TCO).

Virtualizing applications or services means installing and running an application or service using virtual machines on a physical computer; the physical computer is running a host operating system as well as a virtual or guest operating system to implement the virtual machines. The virtual machine runs its own operating system, which can either be migrated to a later operating system or, for short-term solutions, can be the same operating system as that used before virtualization.

Virtualization takes consolidation to a new level, breaking the 1:1 relationship between application and server. Virtualization is a consolidation technique that yields additional benefits by abstracting the applications from the physical server and placing them on virtual machines (VMs), many of which can reside on a single physical host. This requirement calls out the virtualization best practices highlighted in the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx). Additional guidance for using virtualization in the context for development and test can be found in the [Windows Server System Architecture Virtual Environments for Development and Test](http://www.microsoft.com/technet/solutionaccelerators/wssra/ve/default.mspx) guide.

## Phase 1: Assess

The goal of the Assess phase again is to take an inventory of the applications, services, and infrastructure in your organization. You may have generated such an inventory already for other requirements in the Infrastructure Optimization Model. [Systems Management Server (SMS) 2003 Inventory](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx) can also be used to inventory the server applications and infrastructure in your organization. Additionally, you will need to [collect software usage information](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_2019.mspx) for use in the Identify phase.

## Phase 2: Identify

After you have generated another inventory of applications and services with corresponding usage details, the Identify phase will analyze the information to determine which applications or services are candidates for virtualization. You should identify the applications or services, especially those requiring limited system resources, on older hardware or non-standard operating systems and applications. Some of the key points to remember when identifying your initial virtualization candidates are described in the following sections.

### Infrastructure Reduction

In this case, you are identifying where hardware can be consolidated by running multiple applications or services using virtual machines on a single host operating system and single piece of hardware. Virtual machines are still isolated from one another as with physical infrastructure, but you can increase overall system utilization, reduce the number of physical systems to manage, and reduce facility requirements, such as floor space, rack space, power, and cooling.

### Hardware Independence

If an application or service is running on hardware that is currently obsolete, this may be a good candidate for virtualization. If the application or service does not warrant the investment to be updated for newer hardware, virtualization may be an excellent option to mitigate this expense by continuing to run a virtual machine form of the obsolete hardware on a newer computer.

### Software Independence

As with hardware independence, the virtual machine can continue to run on an older operating systems and with older applications. This option should only be used when the investment to upgrade the operating system or applications is unwarranted or unfeasible as there are many security, maintenance, and support trade-offs for allowing this standardization exception to continue.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase defines the planning goals, options, and processes for consolidating and migrating application servers onto virtual machines. The following sections briefly explain evaluation and planning relevant to your virtualization strategy; this guidance is derived from the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaplg.mspx).

### Development of Strategies for Consolidation Through Virtualization

The consolidation strategy should be based on your goals and a comprehensive assessment of your environment, requirements, options, and potential impacts, including the following factors:

* Results of the analysis of each application and server, including all characteristics that are relevant to determining consolidation options.
* Consolidation options available for each application, and the advantages and disadvantages of each option.
* Any service-level impacts related to each application (including any mitigation techniques for minimizing the impact on the changed run-time environment).
* Impacts of an application on the business unit, including mitigation techniques for minimizing impacts on application owners.
* IT organization impacts related to each application (including those related to domains, networks, server, storage, applications, and clients).
* End-state impacts for each consolidated application (focusing on the virtual machine environment).
* The security impacts for each consolidated application (especially any mitigating factors related to running applications in virtual machines).

These factors are critical to determining the appropriate consolidation strategy for your organization.

### Operations Management Planning

Consolidation of application servers typically requires improvements in operational processes to offset the technical complexities and operational risks associated with consolidation, with special consideration required for the impacts of running applications in virtual machines. There are operational planning areas directly affected by consolidation and virtualization. Ensuring proper management of these areas requires stringent analysis and frequently requires modifications to operational processes.

#### Backup and Restore Strategies

When applications or services are consolidated using virtual machines, you need to consider not only the backup and restore strategies for the application servers running on the virtual machine, but also the backup and restore strategies for the host operating system and Virtual Server.

#### Change and Release Management

The change and release management plan should address the physical server and host operating system, as well as the virtual machines being deployed. The goals of effective change and release management should include:

* Minimizing service downtime and changes to the user configuration.
* Providing a smooth transition to the production environment.
* Meeting all business objectives.

A good design and management plan can help ensure that these goals are met.

#### Monitoring

Planning for effective monitoring of a virtual machine environment requires real-time assessment and response to application-specific issues. In general, this requires completion of the following planning tasks:

* Agreeing on what the monitoring requirements are.
* Identifying and deploying appropriate processes and technologies for monitoring the host operating systems and guest operating systems.
* Deciding how to optimize the performance of the processes and technologies.
* Putting plans in place that provide for performing continuous monitoring of the infrastructure, as well as turning monitoring off and on when necessary.

#### Service Support

Service support includes the processes, procedures, tools, and personnel that identify, assign, diagnose, track, and resolve incidents, problems, and requests within the approved SLA. During consolidation, the key objectives of support resources are to ensure that the business goals of consolidation are met and that the incidents and problems are resolved quickly.

#### Service Optimization

Service optimization includes defining optimization requirements to be included in the SLA, managing capacity and availability, managing service continuity, managing staff, and financial planning to ensure that the cost of consolidation is justified and budgeted.

### Deployment Planning

Effective planning for a consolidation solution using virtualization requires not only establishing appropriate consolidation, virtualization strategies, and operations plans, but also defining processes for testing, piloting, and rolling out the solution. This effort includes deciding how, when, and where to implement the solution, as well as how to roll back the solution, if required, at any phase of the implementation. Deployment planning should include:

* Testing
* Pilot program
* Rollout programs
* Rollback methods

### Creation of Logical and Physical Designs

The design of each instance of the virtualization technology and the platform on which it resides should include designing for reliability, availability, security, and scalability. It should address both the operations environment and infrastructure considerations. The creation of logical and physical designs should include:

* Domain infrastructure design
* Server sizing and performance
* Virtual machine design
* Server mapping

### Evaluation and Planning Summary

The evaluation and planning guidance included a high- level overview of the tasks required to plan for the consolidation of application servers onto virtual machines; these are typically the initial services that are consolidated and migrated using virtualization technologies.

### Virtual Server 2005

Microsoft Virtual Server 2005 provides server virtualization features described above that support the complex requirements of enterprise server applications and administration.

For more information about Microsoft Virtual Server 2005, visit: <http://www.microsoft.com/technet/prodtechnol/virtualserver/default.mspx>

## Phase 4: Deploy

The intent of this requirement in the Core Infrastructure Optimization Model is to have the plan in place for consolidation of IT services and applications using virtualization technologies. For guidance on deploying virtualization to consolidate applications using Microsoft Virtual Server 2005, see the [Solution Accelerator for Consolidating and Migrating LOB Applications: Implementation Guide for the Virtual Server 2005 Solution](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaimg.mspx).

## Further Information

For more information, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “virtualization.”

To see how Microsoft implements virtualization, go to <http://www.microsoft.com/technet/itshowcase/content/virtualserver2005twp.mspx>.

## Checkpoint: Server Consolidation and Virtualization

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried all IT services and applications in your organization, including performance and traffic data. |
|  | Developed a plan to consolidate server infrastructure by implementing virtual machine technologies. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Server Consolidation and Virtualization capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for server consolidation and virtualization addressed in the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Desktop,_Device_9).

# Requirement: Layered Imaging for Desktops

## Audience

You should read this section if you do not have a layered-image strategy for managing your desktop images.

## Overview

In *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized,* you read about creating, deploying, and maintaining standard images for desktops, and the three approaches to creating disk images—thick, thin, and hybrid. Creating a thick image is a viable approach for standardizing image deployment, but using a thin or hybrid image can increase efficiency and reduce deployment and maintenance costs.

The layered-image approach advocates the thin and hybrid image strategies, meaning that only the OS itself or OS with limited standard core applications is deployed to target machines. Supplemental applications, drivers, or language packs are added via an installation sequence separate from the main image at deploy time. The impact of this is that there are fewer core images to maintain and more flexibility for adding components outside the core image at deployment. To help with determining and implementing image strategies, the [Business Desktop Deployment (BDD) 2007 Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx) discusses the options for desktop imaging and goes into detail for creating desktop images using Microsoft technologies.

For more information on the cost benefits of consolidating images, read the [Optimizing Infrastructure: The Relationship between IT Labor Costs and Best Practices for Managing the Windows Desktop](http://whitepapers.zdnet.com/whitepaper.aspx?docid=284982&promo=100202) white paper.

## Phase 1: Assess

The Standardized level in Core Infrastructure Optimization requires a standard image strategy and a maximum of two desktop operating system versions. In most cases, organizations that have achieved standard images are using techniques for sector-based imaging, or taking a snapshot of a known well-configured machine with all the required applications, components, and settings.

In the Assess phase, you are looking for the number of standard images actually maintained by the organization. This includes anything developed for foreign language operating systems, various hardware abstraction layer (HAL) types, or images maintained for certain unique services in the organization, such as call centers or media labs. You should catalog the components of every image and, during the Identify phase, seek threads of commonality among these images to identify how to get to a thinner and more consolidated set of desktop images. To automate the gathering of software, hardware, and OS information on machines used currently for standard image capturing, it is recommended to use the [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx), [SMS 2003 hardware and software inventory](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx), or the [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625).

## Phase 2: Identify

In the Identify phase, you should look at the common elements of the images cataloged. Thin or layered images may not be the best solution in every operation of your organization, but there are several distinct benefits to having thinner images; these are discussed in the next phase. Certain limiting factors, such as platform type (x64 or x86) or multiple HAL-types when using Windows XP or earlier operating systems, will force you to maintain multiple images. These limitations are relieved somewhat with Windows Vista, where one image can support multiple HAL-types, but unique images are required for x86 and x64 platforms.

The requirement for layered images drives toward further image consolidation, which will reduce overall maintenance requirements for managed images. Using your catalog of standard images, isolate where the opportunities are in order to consolidate operating systems as much as possible. This can start with things like standardizing on a single language core OS with Multilingual User Interface (MUI) packs or opting for a language-neutral OS with add-on language packs.

After consolidating language versions, examine the applications, if any, required for every user in the organization; these can include such items as antivirus applications, productivity suites, or special LOB applications required as standard applications on every user’s machine in the organization. Then look for the applications that can be packaged and available for installation sequences after the core thin images are installed; these can be LOB applications unique to certain departments, such as foreign language software used in limited locations. Once you have isolated the candidates for the core image and those components that can be added as layers after the core image installation, you are ready to begin evaluating how to incorporate a layered-image strategy into your organization.

## Phase 3: Evaluate and Plan

Now that you have identified the commonalities of your managed images and isolated opportunities to further consolidate images and move closer to a layered-image approach, you are ready to begin evaluating and planning where it makes the most sense to use the layered-image approach in your organization and where it isn’t possible. After evaluating the appropriate usage of layered images in your organization, you can begin planning for the transition. The following sections define the possible image types and discuss the advantages of layered images to help evaluate the best strategy for your organization.

### Thick Images

Thick images contain the operating system, applications, and other corporate standard files. When you use a thick image, everything is loaded onto the client computer in one step. The disadvantage of thick images is that all computers receive the same configuration.

### Layered Images

Thin images contain few if any applications. Applications are installed individually on the client computers. Thin images allow flexibility in customizing each client computer, but deployment time increases significantly.

A hybrid image approach combines the benefits of thick and thin image approaches. You create a baseline image consisting of the operating system and any company-standard applications and corporate data files that are used on a majority of desktops within your organization. You then create secondary images that contain applications and data files that are specific to the various organizations that you support. For more information on image types, go to <http://technet2.microsoft.com/WindowsServer/en/library/b5a36970-0de1-4386-a824-529b0272a3171033.mspx?mfr=true>.

### Advantage of Layered Images

Layered images have several advantages over both thick images. These are:

* Deployment time.
* Maintenance.
* Flexibility.

#### Deployment Time

Deployment of layered images represents a compromise between thick and thin image deployment. Loading two layered images takes slightly longer than a single thick image, but it is considerably faster than loading a thin image and numerous applications. Planning the deployment is also simplified. Your focus is on organizational deployment rather than on individual computers.

#### Maintenance

You have several areas to consider in image maintenance. The first is image creation and storage. Another is image content patching and updating.

Depending on the number of operating systems and application versions you must support, you could have numerous distinct thick images to create, store, and maintain. You need to rebuild an entire image each time there is an update to any single component of the image.

When using a layered-imaging strategy, you will need to create and store fewer thin images, and updates are simplified because you have only the operating system and a few applications to patch. All other applications must be updated on each computer on which they are installed. This is far more time consuming than updating and redeploying a layered application image.

Hybrid images combine the benefits of thick and thin images. You need to build fewer overall images, and updates need be applied only to the images that contain the application to be updated. You can then deploy a smaller image to fewer systems.

#### Flexibility

You have far greater flexibility in planning and deploying layered images than you do with the thick image approach. You can customize your disk images based on organizational structure, system configurations, data security needs, and many other criteria that match your organization’s needs.

### Planning and Building Standard Images

Once you have determined the right level of core applications and components to be added into the core operating system image and which applications will be installed outside the operating systems image, it is time to begin building standard desktop images. The process outlined in BDD 2007 contains four primary steps for building images using the BDD 2007 Deployment Workbench console in conjunction with the ImageX command-line imaging utility. Desktop imaging is an iterative process focused on creating, testing, and revising images until they are determined to be stable for deployment. The four key steps in this process are described below in conjunction with the [Computer Imaging System Feature Team Guide in BDD 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx).

#### Add Applications to a Distribution Share

As a first step, you will add applications, including hardware-specific applications, and specify dependencies between applications to a distribution share. These components will be used to create or configure builds in the following step.

#### Configure Builds

Builds are operating system configurations that include unattended setup answer files and, in the case of layered images, a task sequence. Builds associate an operating system with a configuration and contain the tasks required to take place outside the operating system deployment. A task sequence should be defined in a task sequencing engine or, in some cases, via scripting for required pre- and post-installation routines.

#### Configure Deployment Points

Deployment points contain a subset of the distribution share’s source files and builds; they also specify how to install the builds they contain. Updating a deployment point generates the images necessary to connect to the deployment point and begin installation.

#### Capture Operating System Images

The final step associated with desktop imaging is the image capture of the reference computer. You will specify whether to prompt for image capture when creating a build in Deployment Workbench. Then, the process will ask whether to capture an image of the reference computer during the initial interview.

## Phase 4: Deploy

Image deployment is not covered in the imaging process. Refer to the requirement of [Automated Operating System Distribution](#_Automated_Patch_Distribution) at the Rationalized level in Core Infrastructure Optimization.

## Further Information

For more information on layered images, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “layered imaging.”

To see how Microsoft has simplified disk imaging with Vista, go to <http://www.microsoft.com/technet/itshowcase/content/vistadeploy_twp.mspx>.

## Checkpoint: Layered Imaging for Desktops

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried and rationalized the current set of managed desktop images in your organization. |
|  | Developed and implemented a strategy to consolidate desktop images by using thin or hybrid layered imaging for desktop deployment. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Layered Imaging for Desktops capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practices for layered disk images addressed in the [Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx) found in [BDD 2007](http://www.microsoft.com/technet/desktopdeployment/bddoverview.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Security_and).

Capability: Security and Networking

# Introduction

Security and Networking is the third Core Infrastructure Optimization capability. The following table describes the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Security and Networking.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  Multi-layered security models are not deployed across the network—from perimeter, through firewall, server, desktop, and application levels  Firewall is not a standard component of desktops  Mobile users lack secure access to resources through the routing infrastructure provided by a public network  **IT Challenges**  Servers accept inbound traffic from any host, increasing vulnerability to attacks  Weak authentication of wireless clients  Weak encryption and data integrity of wireless LAN | **Projects**  Deploy policy-managed firewalls on servers. Secure remote access to internal resources and LOB applications  Provide secured and guaranteed communication verification between servers  Implement SLA monitoring and reporting for servers  Implement secure communication mechanism for presence  Deploy Active Directory and IAS/RADIUS for wireless network authentication and authorization  Implement centrally managed certificate services  Begin to proactively manage bandwidth to branch offices | **Business Benefits**  Users have secure access to resources regardless of location  Proactive policies and processes for security, configuration, and management increase stability  **IT Benefits**  Improved asset management of hardware and software for desktops  Centralized group policies to distribute IPsec policies and filters, increasing the level of security on PCs  IPsec policies increase the security of network environments by limiting inbound traffic to trusted hosts  IT spends less time managing crises and more time delivering new services to the business |

The Rationalized Level in the Infrastructure Optimization Model addresses the key areas of networking and security components, including: local firewalls, IP security, availability monitoring, securing wireless infrastructure, certificate management, and WAN management.

# Requirement: Policy-managed Firewalls on Servers and Desktops

## Audience

You should read this section if you do not have a policy-managed firewall on at least 80 percent of your servers and desktops.

## Overview

In *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized,* you read about protecting network computers by using a centralized perimeter firewall. To move from the Standardized level to the Rationalized level, you need to supplement your network’s firewall protection by establishing and enforcing policies on your servers *and* desktops using class 1 host-based firewalls. Microsoft and other software vendors offer firewall software that allows you to configure protection based on a policy or set of rules. This requirement is tightly associated with the requirement for [Centralized Directory-based Configuration and Security](#_Requirement:_Centralized_Directory-) also at the Rationalized level.

Most class 1 firewalls can be configured for different levels of protection, from minimal to very restrictive. When you allow users to set the level of protection on their own computers, you cannot be assured that they will select a level that will protect your entire network. With policy-managed firewalls, you can determine the level of security that meets your network needs.

## Phase 1: Assess

In the Assess phase, you are again assessing which computers in your environment already have some form of host-based firewall with policy management capabilities. The Rationalized level stipulates that 80 percent or more of your desktop PCs run either Windows XP SP2 or Windows Vista (see [Requirement: Latest Two OS Versions and Service Packs on Desktops](#_Requirement:_Latest_Two)); there is no stated requirement at the Rationalized level that servers run the latest two operating systems. This is important because, assuming your organization has deployed the latest two desktop operating system versions, you will have already met the requirement of having host-based firewall features available on desktops, and you will simply need to incorporate configuration enforcement requirements via Group Policy to ensure that Windows Firewall is running with a desired configuration. Host-based firewalls in Windows Server products began with the release of Windows Server 2003 SP1, so if your organization is not running at least 80 percent of its server infrastructure with Windows Server 2003 SP1 or later, you will need to inventory and identify these systems without a host-based firewall. To automate the operating system and application information on server infrastructure, it is recommended to use [SMS 2003 hardware inventory](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx).

## Phase 2: Identify

Using your server inventory generated in the previous phase, the Identify phase simply isolates the server infrastructure requiring host-based firewalls. In the Evaluate and Plan phase, you will determine the appropriate mitigation strategy to enable host-based firewalls and determine the appropriate firewall configuration to be enforced using Group Policy.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, you will examine host-based firewall technologies and determine the appropriate course of action to have host-based firewalls present on 80 percent of desktops and servers in your organization. After the strategy has been determined for applying host-based firewalls to the majority of your desktops and servers, you should determine how Group Policy can be used to enforce usage and configuration of the host-based firewalls. This phase is only responsible for evaluating and planning for host-based firewall deployment in a test environment. The following sections focus on Windows Firewall, but you may elect to use similar technologies, such as [BlackICE](http://www.digitalriver.com/dr/v2/ec_dynamic.main?SP=1&PN=10&sid=26412) from Internet Security Systems or [Zone Alarm](http://www.zonelabs.com/store/content/catalog/catalog_main.jsp?dc=12bms&ctry=US&lang=en) from Zone Labs.

### Windows Firewall

Windows Firewall is a built-in, host-based, stateful firewall that is included in Windows XP with Service Pack 2, Windows Server 2003 with Service Pack 1, Windows Vista, and Windows Server Code Name "Longhorn" (now in beta testing). Windows Firewall drops incoming traffic that does not correspond to either traffic sent in response to a request of the computer (solicited traffic) or unsolicited traffic that has been specified as allowed (excepted traffic).

As a host firewall, Windows Firewall runs on each of your servers and clients; it provides protection from network attacks that pass through your perimeter network or originate inside your organization, such as Trojan horse attacks, worms, or any other type of malicious program spread through unsolicited incoming traffic.

For more resources on Windows Firewall, go to <http://www.microsoft.com/technet/network/wf/default.mspx>.

Windows Firewall, or similar host-based firewall functionality, on 80 percent of desktops and servers is a requirement. As previously mentioned, other host-based firewall products that you may want to evaluate are [BlackICE](http://www.digitalriver.com/dr/v2/ec_dynamic.main?SP=1&PN=10&sid=26412) from Internet Security Systems and [Zone Alarm](http://www.zonelabs.com/store/content/catalog/catalog_main.jsp?dc=12bms&ctry=US&lang=en) from Zone Labs.

### Getting Host-based Firewalls on Desktops and Servers

Once you have selected your preferred firewall technology for desktops and servers and targeted the hosts in need of firewall capabilities, your next task is to test, configure, and deploy those firewall applications to the test infrastructure. These steps align with best practices observed in this guide for patch management, application compatibility testing, and application deployment, as described in [Patch Management for Servers](#_Patch_Management_for), [Compatibility Testing and Certification of Software Distributions](#_Compatibility_Testing_and), and [Automated Tracking of Hardware and Software for Desktops](#_Automated_Tracking_of). If you have selected Windows Firewall as your single and preferred technology for servers predating Windows Server 2003 SP1, you will need to update targeted servers to Windows Server 2003 SP1 or newer.

### Policy Management of Firewalls

Policy management of the host-based firewall is also required as part of the Rationalized level in Core Infrastructure Optimization. For Windows Firewall users, the key is to simply ensure the firewall service is enabled. This straightforward process is performed via the following steps using Group Policy:

Verify that the Group Policy setting, **Windows Firewall: Prohibit use of Internet Connection Firewall on your domain network**, is either disabled or not configured.

If enabled, this setting prevents anyone, including administrators, from enabling or configuring Windows Firewall. To change this policy setting, use the Group Policy Object Editor to edit the Group Policy objects (GPOs) that are used to manage Windows Firewall settings in your organization.

To modify the Prohibit use of Internet Connection Firewall on your domain network setting

1. Open the Group Policy Object Editor to edit the GPO that is used to manage Windows Firewall settings in your organization.
2. Click Computer Configuration, click Administrative Templates, click Network, and then click Network Connections.
3. In the details pane, double-click the **Windows Firewall: Prohibit use of Internet Connection Firewall** on your domain network policy setting.
4. Select either the **Disabled** or **Not Configured** check box.

If you are not using Windows Firewall, locate the equivalent setting for the selected host-based firewall and perform the equivalent procedure. Once completed for at least 80 percent of managed clients and servers, this attribute of the requirement for Policy-managed Firewalls on Servers and Desktops is completed. For more information on Group Policy, see the requirement for [Centralized Directory-based Configuration and Security](#DSDOC_BKMK_TOOLS88f80cb7_d44f_47f7_a10d_) in this guide.

For more information on advanced Windows Firewall settings, see [Best Practices for Managing Windows Firewall](http://technet2.microsoft.com/WindowsServer/en/library/985a4443-4db7-4cce-b523-fd7414fe01271033.mspx).

## Phase 4: Deploy

As a result of the previous three phases, you should be ready to deploy your selected host-based firewall technology and enable policy management. Again, the deployment process encompasses the equivalent best practice recommendations for patch management, application compatibility testing, and application deployment, as described in [Patch Management for Servers](#_Patch_Management_for), [Compatibility Testing and Certification of Software Distributions](#_Compatibility_Testing_and), and [Automated Tracking of Hardware and Software for Desktops](#_Automated_Tracking_of). Refer to those requirements for detailed information about the planning and deployment process.

## Further Information

For more information on firewalls, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “Windows Firewall.”

To see how Microsoft incorporates firewalls into network perimeter security, go to <http://www.microsoft.com/technet/itshowcase/content/secnetwkperim.mspx>.

## Checkpoint: Policy-managed Firewalls on Servers and Desktops

|  |  |
| --- | --- |
| X | Requirements |
|  | Inventoried your desktop and server computers to identify which hardware currently has host-based firewall technologies. |
|  | Deployed host-based firewall technology to hardware lacking firewall capabilities or updated servers to Windows Server 2003 SP1 or later. |
|  | Established policy enforcement to ensure that host-based firewalls are always enabled and cannot be disabled. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Policy-managed Firewalls on Servers and Desktops capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources outlined in this guide for policy-managed host-based firewalls and in [Best Practices for Managing Windows Firewall](http://technet2.microsoft.com/WindowsServer/en/library/985a4443-4db7-4cce-b523-fd7414fe01271033.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Security_and_1).

# Requirement: Secure Remote Access to Internal Resources and LOB Applications

## Audience

You should read this section if your employees do not have secure remote access to internal resources and LOB applications beyond e-mail—for example, a virtual private network (VPN) or Microsoft Terminal Services.

## Overview

In the current business environment, organizations are under pressure to reduce costs, increase efficiency, and maximize performance from the existing infrastructure. The growth of the Internet, together with new global business opportunities, makes it imperative that organizations provide secure 24x7 network access to employees and locations around the world. Two scenarios in which remote access is typically used are:

* **Remote client access.** Remote clients are usually single computers, such as home computers or laptops of employees who need to access enterprise resources while working at home or traveling.
* **Site-to-site access.** Site-to-site access is used between branch offices and centralized facilities of the organization to access resources and data at different logical and physical locations.

Both of these key remote access requirements of an enterprise organization can be provided using a VPN. Both of these solutions require the underlying presence of either a dial-up connection or an Internet (shared) leased-line connection. This guide focuses on VPN and introduces Terminal Services to fulfill the requirement. Guidance is based on [Windows Server System Reference Architecture (WSSRA) Remote Access Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/remoteaccessservices/default.mspx).

For more technical resources on VPN in Windows Server 2003, visit the [Virtual Private Networks Web site on Microsoft TechNet](http://www.microsoft.com/technet/network/vpn/default.mspx).

## Phase 1: Assess

During the Assess phase, you should identify the current ways your user base is working from remote locations. Organizations often only provide access to e-mail via services such as Microsoft Office Outlook® Web Access (OWA) or Web-enabled line-of-business applications. In these cases, end users effectively have a subset of functionality compared with those on-site. In the Assess phase, you should determine the high-level list of services available to users on-site, such as Intranet and collaboration services, and those available to users off-site or in branch offices, such as Web-based e-mail and LOB applications.

## Phase 2: Identify

Now that you have the list of services for on-site and off-site or branch office users, the Identify phase simply determines which services offered on site would increase user productivity and effectiveness if securely delivered through remote access to off-site users. Typically, the key remote access requirements of an organization, namely remote client access and site-to-site access, can be provided using a VPN. Both of these solutions require an Internet connection or a leased-line connection.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase examines how the selected remote access services are delivered, along with controls used to maintain security. For most organizations, it would be too costly to open an office in every city or to provide private circuits to every employee’s home to ensure secure connections to the enterprise network. A VPN enables business partners and employees to make secure, encrypted connections using the Internet, usually at a lower cost.

### Virtual Private Networks

A virtual private network (VPN) is a secure, encrypted connection between two endpoints that is established over a shared connection such as the Internet and used as an extension of an enterprise network. A VPN enables the organization to use the existing global Internet infrastructure by simply connecting an office or user to an Internet service provider (ISP). VPN is also an extensible technology; for example, Voice over IP (VoIP) can be implemented to allow remote users to use their office telephone extension (with all of its messaging capabilities) wherever they may be working at the time.

VPN connections allow users who work at home or travel to obtain a remote access connection to an organization server, using the infrastructure provided by a public internetwork such as the Internet. From the user's perspective, the VPN is a point-to-point connection between the computer, the VPN client, and an organization server (the VPN server). The exact infrastructure of the shared or public network is irrelevant because it appears as if the data is sent over a dedicated private link.

VPN connections also allow organizations to have routed connections with other organizations over a public internetwork such as the Internet while maintaining secure communications, for example, for offices that are geographically separate. A routed VPN connection across the Internet logically operates as a dedicated wide area network (WAN) link.

The following diagram depicts an architectural design for remote access services using VPN.

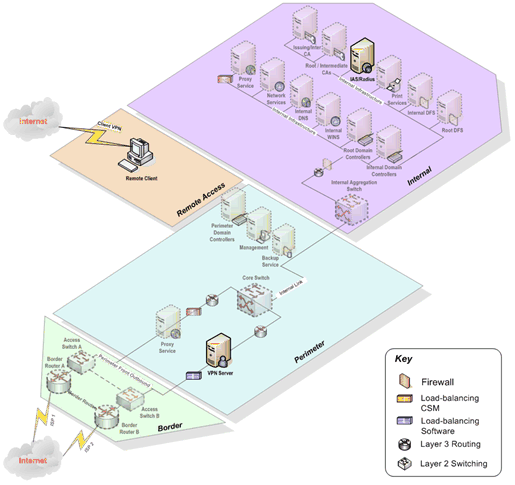


Figure 7. Architectural design for remote access services using a VPN

### VPN Design Considerations

There are many issues that need to be considered when designing a VPN solution, including security, costs, integration, future requirements, and administration. Before deciding on the appropriate VPN technology, it is important to determine the design goals for a VPN solution. These goals differ depending on whether the solution is for client remote access, site-to-site access, or both. For more information about VPN design options, see the [WSSRA Remote Access Services Blueprint](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/RemoteAccessServices/igrabp_2.mspx).

### Planning for Remote Access Services

The remote access design is based on information gathered during the process of determining the business and technical requirements. Typically, a remote access solution is necessary for remote clients, such as employees working at home or while traveling, and branch office sites with multiple users, where business class site-to-site connections exist.

For detailed information on planning remote access services to remote clients, read [WSSRA Remote Access Services Planning Guide for the Corporate Data Center (CDC) Scenario](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/RemoteAccessServices/igrapg_2.mspx).

For detailed information on planning remote access services to branch offices, read:

* [WSSRA Remote Access Services Planning Guide for the Satellite Branch Office (SBO) Scenario](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/RemoteAccessServices/igrapg_3.mspx)
* [Virtual Private Network Design for the Branch Office Infrastructure Solution](http://www.microsoft.com/technet/solutionaccelerators/branch/biosv2_43.mspx)

### Terminal Services

The Terminal Services component of Microsoft Windows Server 2003 lets you deliver Windows-based applications, or the Windows desktop itself, to virtually any computing device—including those that cannot run Windows.

Terminal Services in Windows Server 2003 provides three important benefits for secure remote access:

* Rapid centralized deployment of applications.
* Low-bandwidth access to data.
* Windows anywhere.

For more information on Terminal Services, go to <http://technet2.microsoft.com/windowsserver/en/technologies/featured/termserv/default.mspx>.

## Phase 4: Deploy

After evaluating your options for remote access services and planning for what is required to provide appropriate service to remote clients and branch offices, the implementation of your design occurs in the Deploy phase. The [WSSRA Remote Access Services Build Guide](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/RemoteAccessServices/igrabg.mspx) provides implementation steps for testing and deploying VPN services to remote clients in the CDC scenario and to branch offices in the SBO scenario.

## Further Information

To see how Microsoft implements VPN and Terminal Services, go to the following Web sites:

* <http://www.microsoft.com/technet/itshowcase/content/isa2004sp2.mspx>
* <http://www.microsoft.com/technet/itshowcase/content/rasecwp.mspx>

## Checkpoint: Secure Remote Access to Internal Resources and LOB Applications

|  |  |
| --- | --- |
| X | Requirements |
|  | Evaluated remote access requirements for remote clients and branch offices. |
|  | Designed and implemented secure virtual private network or similar services to remote clients and branch office. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Secure Remote Access to Internal Resources and LOB Applications capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for VPN found in the [Virtual Private Networks Web site on Microsoft TechNet](http://www.microsoft.com/technet/network/vpn/default.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Security_and_2).

# Requirement: Secured and Guaranteed Communication Verification Between Servers

## Audience

You should read this section if you do not have a secured and guaranteed way to verify communication between critical servers such as domain controllers and e-mail servers.

## Overview

Organizations face increasing challenges in securing the perimeters of their networks. As organizations grow and business relationships change, and customers, vendors, and consultants need to connect mobile devices to your network for valid business reasons, controlling physical access to a network can become impossible. The advent of wireless networks and wireless connection technologies has made network access easier than ever. This increased connectivity means that domain members on the internal network are increasingly exposed to significant risks from other computers on the internal network, in addition to breaches in perimeter security.

The concept of logical isolation this guide presents embodies two solutions: server isolation to ensure that a server accepts network connections only from trusted domain members or a specific group of domain members, and domain isolation to isolate domain members from untrusted connections. These solutions can be used separately or together as part of an overall logical isolation solution.

At its core, server and domain isolation enables IT administrators to restrict TCP/IP communications of domain members that are trusted computers. These trusted computers can be configured to allow only incoming connections from other trusted computers or a specific group of trusted computers. Group Policy centrally manages the access controls that control network logon rights. Nearly all TCP/IP network connections can be secured without application changes because Internet Protocol Security (IPsec) works at the network layer below the application layer to provide authentication and per-packet security, end-to-end between computers. Network traffic can be authenticated, or authenticated and encrypted, in a variety of customizable scenarios. This guide follows guidance and recommendations from the [Server and Domain Isolation Using IPsec and Group Policy Guide on Microsoft TechNet](http://www.microsoft.com/technet/network/sdiso/default.mspx).

## Phase 1: Assess

Consistent with other requirements in this guide, the first phase is about assessing the current state of your organization. The process of obtaining and maintaining a reliable record of an organization's computers, software, and network devices is a classic IT challenge. Information about the following items is required to define the current state:

* Network discovery
* Documentation of network segmentation
* Network infrastructure devices
* Analysis of current network traffic model
* Active Directory
* Host discovery
* Host data requirements

For detailed information on how to gather this information, read the [Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 3: Determining the Current State of Your IT Infrastructure](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch3.mspx). This guide discusses the requirements for each item and how to collect information via automated discovery using [SMS 2003](http://go.microsoft.com/fwlink/?LinkId=69780) or similar products as well as manual discovery options.

## Phase 2: Identify

The Identify phase is about determining which strategies are appropriate for your organization’s needs. Defending a modern IT infrastructure from attackers while simultaneously allowing employees to work in the most agile and productive manner is not an easy task. Simply understanding the wide range of technologies that can help secure an environment is difficult enough for many people. It might help to see exactly where the solution fits within a typical IT infrastructure and how it is designed to complement existing network defenses.

The following figure shows a typical network infrastructure consisting of a number of network defense layers and illustrates where logical isolation fits within a typical environment.

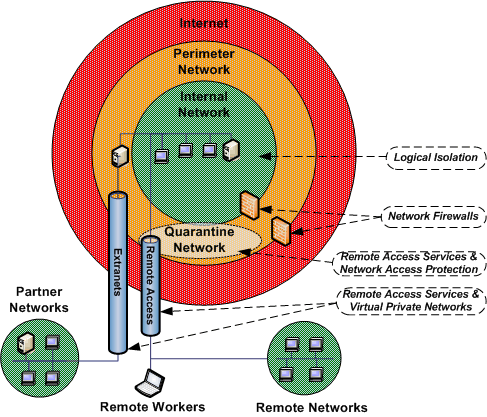


Figure 8. Typical network infrastructure

The outcome of the Identify phase will be to determine the high-level requirements for your Server and Domain Isolation Design. In the Evaluate and Plan phase, we will establish detailed requirements and an execution plan. For more information, see the [Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 4: Designing and Planning Isolation Groups](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch4.mspx).

## Phase 3: Evaluate and Plan

The goal of the Evaluate and Plan phase is to ensure that all options have been considered for securing and guaranteeing verified communication between servers. In this case, we are focusing on IPsec as the mechanism to do this; there is an additional related requirement for [centrally managed certificate services](#_Centrally_Managed_Certificate) at the Rationalized level in the Core infrastructure Optimization Model.

In order to generate an executable plan for the Deploy phase, we provide instructions for implementation of the server and domain isolation design.

### Evaluating Internet Protocol Security

IPsec is typically used to protect the communication channel between two servers and restrict the computers that can communicate with one another. For example, you can help protect a database server by establishing a policy that permits requests only from a trusted client computer, such as an application server or a Web server. You can also restrict communication to specific IP protocols and TCP/UDP ports.

The networking requirements and recommendations for a server farm make IPsec a good option because:

* All servers are contained on one physical LAN (to improve IPsec performance).
* Servers are assigned static IP addresses.

IPsec can also be used between trusted Windows Server 2003 or Microsoft Windows 2000 Server domains. For example, you can use IPsec to secure communication of a Web server or application server in a perimeter network that connects to a computer running Microsoft SQL Server on an internal network. For more information, see [Selecting IPsec Authentication Methods](http://go.microsoft.com/fwlink/?LinkId=76093&clcid=0x409) in the [Windows Server 2003 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409).

For more information about recommended environments for IPsec, see [Determining Your IPsec Needs](http://go.microsoft.com/fwlink/?LinkId=76094&clcid=0x409) in the [Windows Server 2003 Deployment Guide](http://go.microsoft.com/fwlink/?LinkId=76095&clcid=0x409).

### Planning for Server and Domain Isolation

During the Identify phase, we created high-level requirements. The next step is to create an implementation plan using [Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 4: Designing and Planning Isolation Groups](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch4.mspx). After a plan has been created and detailed requirements defined, a combination of the following elements will implement these requirements:

**Inbound and outbound access requirements for the isolation domain and isolation groups:**

* Internet Protocol security (IPsec) policy designed specifically for the isolation group that requires IPsec Internet Key Exchange (IKE) negotiation for inbound and outbound connections.
* Domain-based security groups called network access groups to allow or deny network access when using IPsec-protected traffic.

**Network traffic protection requirements for the isolation domain and isolation groups:**

* IPsec policy filters designed to properly identify which traffic should be secured.
* IPsec filter actions that negotiate the required level of authentication and encryption for the traffic that the filters identify.
* IPsec filter action settings to control whether plaintext communication is allowed when trusted hosts initiate outbound connections.

[Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 5: Creating IPsec Policies for Isolation Groups](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch5.mspx) discusses the preparation of the solution using Group Policy and IPsec policies in Active Directory using Windows Server 2003, and configuration of domain members using Windows Server 2003 and Microsoft Windows XP.

## Phase 4: Deploy

The goal of the Deploy phase is to implement what has been planned as a result of the previous three phases. In this phase you will create IPsec policies in Active Directory, including the creation of filter lists, filter actions, and IPsec policies to implement isolation groups. The following figure depicts the various components of an IPsec policy and how they are associated with each other.

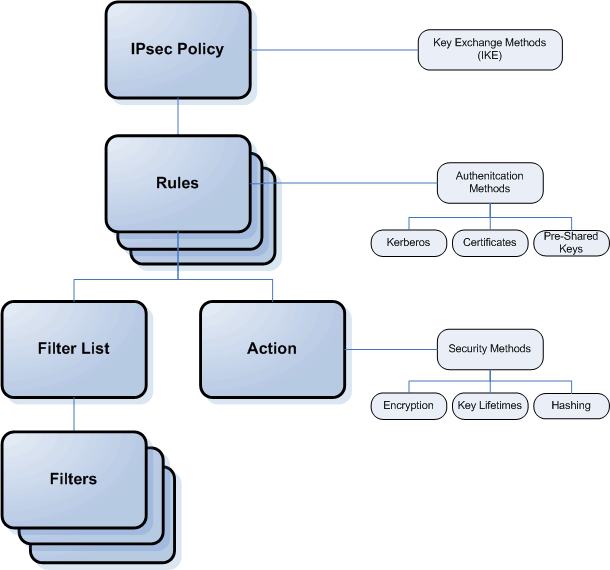


Figure 9. IPsec policy components

For detailed implementation guidance of IPsec policies, read [Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 5: Creating IPsec Policies for Isolation Groups](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch5.mspx).

## Further Information

For more information on IPsec, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “IPsec.”

To see how Microsoft secures communications between servers, go to <http://www.microsoft.com/technet/itshowcase/content/ipsecdomisolwp.mspx>.

## Checkpoint: Secured and Guaranteed Communication Verification Between Servers

|  |  |
| --- | --- |
| X | Requirements |
|  | Assessed the current state of network infrastructure affected by Internet Protocol Security (IPsec). |
|  | Identified organizational requirements to ensure secured and guaranteed communication between servers, including regulation and compliance impacts. |
|  | Developed and implemented a plan across the organization using IPsec to meet defined requirements. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Secured and Guaranteed Communication Verification Between Servers capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for communication between servers.

Go to the [next Self-Assessment question](#_Requirement:_Security_and_3).

# Requirement: Service Level Agreement Monitoring and Reporting for Servers

## Audience

You should read this section if you do not have a service level agreement (SLA) for monitoring and service level reporting for 80 percent or more of your servers.

## Overview

Managing IT using a service management approach is becoming more prevalent in today’s IT industry. As organizations work to stay competitive and meet the needs of their internal and external consumers, they find it necessary to view their IT infrastructures as more than a collection of servers connected through wide area networks (WANs) and running applications You and your organization need to view these resources as services that generate revenue and provide capabilities for your consumers. When you take this approach, you need to understand all of the components making up the services and each component’s impact on the level of availability that the service provides. In addition, you must successfully measure your service delivery over time to clearly understand the quality of service that your systems are providing.

The *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide discussed the requirement of having an automated way of monitoring critical servers in your organization at the Standardized level. At the Rationalized level, we are simply extending the requirement to all servers in the organization and attaching the service level management requirements as part of the monitoring requirement. The Rationalized level does not require a minimum bar for availability; this is determined as appropriate for each IT service in the organization.

## Phase 1: Assess

As with the Standardized level, in the Assess phase your organization should take an inventory of all servers in your organization’s infrastructure. You can manually identify the servers and specifications or use a tool to automate the inventory process, such as the [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx) inventory collection features.

Additional deliverables for moving to the rationalized level are:

* Determining the primary IT services in your organization (service catalog).
* Assigning the infrastructure components necessary for delivering these services.
* Collecting information to determine a baseline current service level.

### Establishing Service Level Baselines

A baseline is a line drawn in time, taking a “snapshot” of the situation. In this instance, it is a picture of the service level management within the organization. A baseline provides a picture of the services being delivered at that specific time and provides a plan for achieving future goals in service level management. Optimizing IT performance requires not only a clear vision of the objective, but also of the current baseline from which the process will begin.

For more guidance on assessing service level baselines, read the [Microsoft Operations Framework (MOF) Service Level Management guidance](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx).

## Phase 2: Identify

After all servers have been inventoried, the Identify phase at the Rationalized level is the process when appropriate services levels are defined against your baselines. The main goal of service level management is to improve the services available to the business in the long term and to resolve service provision issues that currently exist.

Among the many benefits to the IT department, in addition to the improvement of service, is an increased knowledge of business expectations and improved cost management. Service level management allows the IT department to meet business expectations and opens a dialog to confirm these expectations. For example, an IT department may want to deliver a service at a 100 percent, 99.999 percent, or even 70 percent availability, but it may not be able to explain how it arrived at this number. Unless this expectation is documented and agreed on early in the service level management process, the IT department might focus on a non-business–critical service—for example, developing staff, investing in hardware, software, and other costly endeavors—with little real benefit to the business.

### Service Level Objectives

When setting service level objectives, measure what the business is asking for. Often this can include process measurements—for example, rating customer satisfaction, returning phone calls, and responses to queries. There may be ways in which existing technology within the organization can be used to assist in these measurements. For example, call-center technology can run reports that are collated against calls logged at the service desk registering outgoing calls by individuals.

There are often complex component chains that result in the delivery of a service. It is possible, however, to agree on a final objective for the service as long as the service delivery of this objective can be measured over the end-to-end chain of components.

#### Common Measures for Service Level Objectives

|  |  |
| --- | --- |
| Measure | Example |
| Availability | Days and hours the service is available or a % figure based on this. |
| Responsiveness and performance | Speed and volume (throughput or workload measures) of service, time to acquire data, speed of data transfer and response time, and technical and human speed of response. |
| Security | The security of the service. |

The measures for the service level objectives should be carefully considered using the following criteria:

* Do they support the business objectives?
* Are they specific?
* Can they be measured?
* Are they attainable, even if this requires significant effort on the part of IT?
* Are they realistic in relation to the benefit they will bring to the business?

## Phase 3: Evaluate and Plan

With all services defined in a service catalog and desired service levels defined, in the Evaluate and Plan phase we will evaluate technologies to automate monitoring of the components present in the IT service.

### Monitoring Software

This section illustrates how software can be used to monitor the availability of critical servers. In this example, [Microsoft Operations Manager (MOM)](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx) is used in the monitoring role. Whether using MOM or not, software for monitoring availability or other service level measures of servers should have the following functionality:

* Ability to gather server attribute information and to apply specific rules to monitor them, based on their attributes.
* Ability to obtain data from event logs and other providers, as defined by specific rules.
* Ability to collect performance data based on performance counters.
* Ability to generate alerts based on criteria specified in rules.

Depending on the measures defined in your organization’s service level agreements, MOM may be used as the sole technology for collecting data. In most cases, MOM data will need to be augmented with data from other services; for example, if you have defined service levels as part of change and release management, you will need to use status reports from other mechanisms like Systems Management Server 2003 reporting.

System Center Operations Manager 2007 is in the process of being released at the time of this publication. As the next version of an operations management solution from Microsoft, it adds features for service-oriented health monitoring, client monitoring, and domain services monitoring.

#### MOM Availability Management Pack

With the MOM Availability Management Pack you can collect and analyze data from the event logs of your servers and then generate configurable reports that you can view and customize to suit the needs of your organization. You can use these reports to identify the causes for planned and unplanned downtime and take preemptive actions to decrease downtime in the future.

You can use the availability reports to:

* Determine whether your servers are meeting their availability and reliability objectives.
* Filter reports to track trends by viewing information collected over a specific length of time, such as over a period of months or years.
* Identify the best and worst performing computers for a particular area.
* Identify problem areas, such as a particular application or operating system version that stops responding.
* View and analyze information gathered using Shutdown Event Tracker.

The MOM Availability Management Pack can be an invaluable tool that you can use to facilitate key monitoring measures in your service level management and move to the Rationalized level. For more information on the MOM Availability Management Pack, go to <http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/3e1dfa65-84a5-4e3e-9403-3ef9b47c6b68.mspx?mfr=true>.

### Planning for Microsoft Operations Manager Deployment

If you have selected Microsoft Operations Manager as the monitoring technology for your servers and it has not already been deployed in your environment, see the [MOM 2005 Deployment Planning Guide](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/8331b1ef-ce28-4280-9952-ac3e067214b7.mspx) as part of the [Microsoft TechNet Operations Manager TechCenter](http://www.microsoft.com/technet/mom/mom2005_default.mspx).

### System Center Operations Manager 2007

System Center Operations Manager 2007 offers a service-oriented monitoring approach that enables you to monitor your end-to-end information technology services, scale monitoring across large environments and organizations, and use Microsoft application and operating system knowledge to resolve operational problems. Following are some of the rich capabilities that Operations Manager 2007 provides.

#### Service-oriented Monitoring

A consolidated Operations Console displays the health of your environment and allows you to handle alerts. For additional information about the Operations Console, see [Operations Console in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb381361.aspx).

Reports provide multiple ways to view of the health of your environment. For additional information about reporting, see [Reporting in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb309653.aspx).

#### Built-in Management Packs

Out-of-the-box Management Packs provide monitoring information for many Microsoft applications. In addition, you can create your own Management Packs to monitor your custom applications. For additional information about Management Packs, see [Management Packs in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb309695.aspx).

Most Microsoft Management Packs include information about how to resolve common problems with the application.

#### Client Monitoring

Client Monitoring enables you to forward error reports for operating systems and applications to Microsoft and receive solutions for those errors, as available. For additional information, see [Client Monitoring in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb309675.aspx).

#### Active Directory Domain Services

Active Directory Domain Services Integration uses prior investments by allowing you to assign agent-managed computers to Management Groups. For additional information about Active Directory Domain Services, see [Active Directory Domain Services Integration in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb381196.aspx).

#### Secured Monitoring Environment

Security features allow you to monitor the health of information technology services and applications even when parts of the environment are outside your secured area. For additional information about security features, see [Security Considerations in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb309725.aspx) and [Operations Manager 2007 Gateway Server](http://technet.microsoft.com/en-us/library/bb381288.aspx).

Role-based authorization allows you to tailor the actions your operators and administrators can take. For additional information about roles, see [About User Roles in Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb309440.aspx).

Audit collection efficiently collects security events from managed computers and provides reports for analysis. For additional information about audit collection, see [Audit Collection Services (ACS)](http://technet.microsoft.com/en-us/library/bb381258.aspx).

#### Further Information

For more information about System Center Operations Manager 2007, visit <http://www.microsoft.com/technet/opsmgr/opsmgr2007_default.mspx>.

## Phase 4: Deploy

After you have defined the IT services in a service catalog, determined the baseline or current service levels, defined service levels appropriate for your organization, and determined a plan for automating service level monitoring, it is time to implement the availability monitoring solution.

If your organization has selected Microsoft Operations Manager as the technology to perform availability monitoring of your systems, detailed deployment guidance can be found in the [MOM 2005 Deployment Guide](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/b7b0c768-64d1-486e-b9ed-7292c9e545f9.mspx?mfr=true) and [System Center Operations Manager 2007 Deployment Guide](http://www.microsoft.com/technet/opsmgr/2007/library/proddocs.mspx) at Microsoft TechNet.

## Further Information

For more information, go to [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “SLA.”

* For more information on monitoring server availability with MOM 2005, go to <http://www.microsoft.com/technet/prodtechnol/mom/mom2005/Library/faf19f47-facd-4467-9510-e7c84c671572.mspx?mfr=true>.
* For information on additional functionality to optimize server monitoring using MOM 2005, see [Solution Accelerator](http://www.microsoft.com/technet/solutionaccelerators) content.
* [Notification Workflow](http://go.microsoft.com/fwlink/?LinkId=33856&clcid=0x409). Notification Workflow is a Microsoft SQL Server-based notification services application that can be used to extend notification functionalities of MOM 2005.
* [Autoticketing](http://go.microsoft.com/fwlink/?LinkId=33876&clcid=0x409). Autoticketing provides guidance for automated ticket generation, enabling the automated posting of a request (or ticket) into the Trouble Ticketing (TT) system used for incident management.
* [Alert Tuning Solution](http://go.microsoft.com/fwlink/?LinkId=33861&clcid=0x409). Alert Tuning helps reduce the volume of alerts when deploying MOM 2005 management packs.
* [Service Continuity](http://go.microsoft.com/fwlink/?LinkId=33874&clcid=0x409). Service Continuity helps maintain the availability of MOM 2005 service.
* [Multiple Management Group Rollup](http://go.microsoft.com/fwlink/?LinkId=33875&clcid=0x409). Multiple Management Group Rollup allows a business to propagate data from multiple management groups into one data warehouse to create consolidated and aggregated reports.
* To see how Microsoft monitors Exchange Server 2003, go to <http://www.microsoft.com/technet/itshowcase/content/monittsb.mspx>.
* To see how Microsoft uses service level agreements, go to <http://www.microsoft.com/technet/itshowcase/content/itscorecdnote.mspx>.

## Checkpoint: Service Level Agreement Monitoring and Reporting for Servers

|  |  |
| --- | --- |
| X | Requirements |
|  | Defined your organization’s IT services in a service catalog. |
|  | Determined the baseline or current service levels for defined services. |
|  | Defined service levels appropriate for your organization and determined a plan for automating service level monitoring. |
|  | Implemented an automated availability monitoring solution. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for SLA Monitoring and Reporting for Servers capabilities of the Core Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for establishing and monitoring server SLAs in [Microsoft Operations Framework](http://www.microsoft.com/mof).

Go to the [next Self-Assessment question](#_Requirement:_Security_and_4).

# Requirement: Secure Communication Mechanism for Presence

## Audience

You should read this section if you do not provide a secured communication mechanism, such as Session Initiation Protocol (SIP), for presence.

## Overview

Presence is real-time information that describes a particular user’s location and availability to communicate. Establishing enterprise-wide presence can provide a significant increase in productivity. Collaboration and communication between workers is more efficient when the tracking time is reduced.

Online presence gives individuals the ability to identify who is online and available to communicate with them at any given moment. Enabling online presence (and installing the required software) adds an online status indicator next to an individual's name wherever his or her name appears in a site collection. The online status indicator shows whether the individual is offline or is online and available to respond to queries via an instant messaging client. When an individual is online, you can click the online status indicator to send an instant message. This direct access to knowledgeable sources can help team members work more effectively and efficiently.

You can take steps to provide secure communications for presence information. Instant messaging systems can provide secure communications between user objects in your directory. By providing technology like Session Initiation Protocol (SIP) for presence communications, you can move from the Standardized level to the Rationalized level. The Rationalized level requires that communication via SIP is also secure; this means that the communication is archived, operated through the directory service, and certificates are used.

To find out more about the business value of presence, download the [Live Communications Server 2005 Document: Business Value of Presence](http://www.microsoft.com/downloads/details.aspx?FamilyId=E297AA65-150E-4B9F-93E9-A313B7988A0E&displaylang=en) document.

## Phase 1: Assess

During the Assess phase we will examine how users in your organization are currently identifying the presence of other users. Many organizations use instant messaging technologies offered by Internet service providers. While enabling online presence is beneficial in many environments where collaboration is critical, it is important to balance the benefits of increased collaboration among group members with the requirements for security and compliance, particularly in regard to the deployment of an instant messaging client. Planning for presence should include assurance that both internal and external communications to and from the instant messaging client are consistent with company-wide policy for security and compliance with regulatory guidelines and business practices. In many organizations, instant messaging conversations must be retained in accordance with record-keeping requirements for electronic communications. For example, organizations subject to Sarbanes-Oxley regulation must archive instant messaging conversations as a part of their records-retention requirements.

The primary deliverable for the Assess phase is to take an inventory of software applications currently used in your organization to enable presence and instant messaging. In highly locked-down environments, your users may be policy-restricted from installing applications; nonetheless, it is still recommended that you take an inventory of all systems. You can centrally inventory your environment with tools such as [Systems Management Server 2003](http://www.microsoft.com/technet/sms/default.mspx) or the [Application Compatibility Toolkit (ACT)](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx).

## Phase 2: Identify

During the Identify phase, you will begin to gather the high-level requirements for enabling presence in accordance with regulations or organizational policies. As stated above, for many organizations it is imperative to archive instant messaging conversations in-house. Additionally, you will want to investigate the extent to which presence indicators are integrated into other productivity applications, such as e-mail and collaboration software. The requirements specification resulting from the Identify phase will be used when evaluating and planning for presence in the following phases.

For information how presence is used with Microsoft Office SharePoint® Server, see <http://technet2.microsoft.com/Office/en-us/library/3f53f3d3-85b8-42e5-8213-afb5eec7e8651033.mspx>.

For information on integrating presence functionality with Microsoft Office Outlook, see <http://technet2.microsoft.com/Office/en-us/library/53c024e4-db55-4858-9ef6-5cba97c1afbd1033.mspx>.

## Phase 3: Evaluate and Plan

During the Evaluate and Plan phase, you will examine the technologies specific to enabling presence in your environment. The following sections highlight the protocol and list some of the Microsoft technology possibilities to enable presence.

### Session Initiation Protocol (SIP)

Session Initiation Protocol (SIP), which is similar to HyperText Transfer Protocol (HTTP), is a text-based application-layer signaling and call control protocol. SIP is used to create, modify, and terminate SIP sessions. It supports both unicast and multicast communication. Because SIP is text-based, implementation, development, and debugging are easier than with H.323. Using SIP, one user can explicitly invite another to join a conversation or multimedia session. A SIP session begins when the second user accepts the invitation. SIP also supports inviting additional users to an already established session.

To learn more about real-time communication protocols, go to <http://www.microsoft.com/technet/prodtechnol/winxppro/plan/rtcprot.mspx>.

### Live Communications Server

Live Communications Server 2005 delivers instant messaging (IM) and presence as part of a scalable, enterprise-grade solution offering enhanced security, seamless integration with other Microsoft products, and an extensible, industry-standard development platform. Microsoft Office Live Communications Server 2005 can provide the following secure communication and collaboration tools and features utilizing SIP for presence:

* Instant messaging
* Audio and video communication
* Data collaboration

Visit the [Microsoft Office Live Communications Server TechCenter](http://www.microsoft.com/technet/prodtechnol/office/livecomm/default.mspx) to find planning, deployment, and operations information for Microsoft Office Live Communications Server.

### Office Communicator 2005 and Office Communicator 2007

Office Communicator 2005 and Office Communicator 2007 are secure enterprise messaging clients that integrate instant messaging with telephony and video for unified instant messaging. Office Communicator 2007 provides integration capabilities with programs across the 2007 Microsoft Office system—including Microsoft Word, Excel®, PowerPoint, OneNote, Groove, and SharePoint Server.

For more information about Office Communicator 2005, see the [Office Communicator 2005 Resource Center](http://office.microsoft.com/en-us/help/HA011992481033.aspx).

For more information about Office Communicator 2007, see [Microsoft Office Communicator 2007 product overview](http://office.microsoft.com/en-us/communicator/HA102037151033.aspx).

### Office Outlook 2007

If your organization is using Microsoft Office Outlook 2007, you can enable presence as part of the contact details information for users in your global address list. When configured, presence is also displayed in received e-mail messages. Office Outlook 2007 can be integrated with Office Communicator 2005 or Office Communicator 2007.

For more information about configuring Office Outlook 2007 to enable presence, see <http://technet2.microsoft.com/Office/en-us/library/53c024e4-db55-4858-9ef6-5cba97c1afbd1033.mspx>.

### Office SharePoint Server 2007

If your organization is using Microsoft Office SharePoint Server 2007, online presence can be enabled for individuals who have access to the SharePoint site to see which other participants are online and to send instant messages to them. Online presence can be a powerful collaboration tool that helps site members to quickly find out who is available to answer questions.

For more information about planning for presence integration in Office SharePoint Server 2007, see the Planning [and architecture for Office SharePoint Server 2007 guide](http://technet2.microsoft.com/Office/en-us/library/5c9d5c10-a7a8-43d1-ac36-a6f50f2d0cd11033.mspx),

### Planning for Presence and Managed Instant Messaging Infrastructure

Once you have evaluated the technologies to enable presence in your organization, the next task is to plan and architect the selected infrastructure. To enable integrated presence within your organization, you will typically require the following:

* Directory service
* Global catalog
* DNS deployed and correctly configured
* Public Key (PKI) and certification authority (CA) infrastructures
* Backend database

By reaching the Rationalized level, these component requirements will typically already be in place in your organization. The following diagram provides sample architecture for Live Communications Server 2005 Enterprise Edition infrastructure.

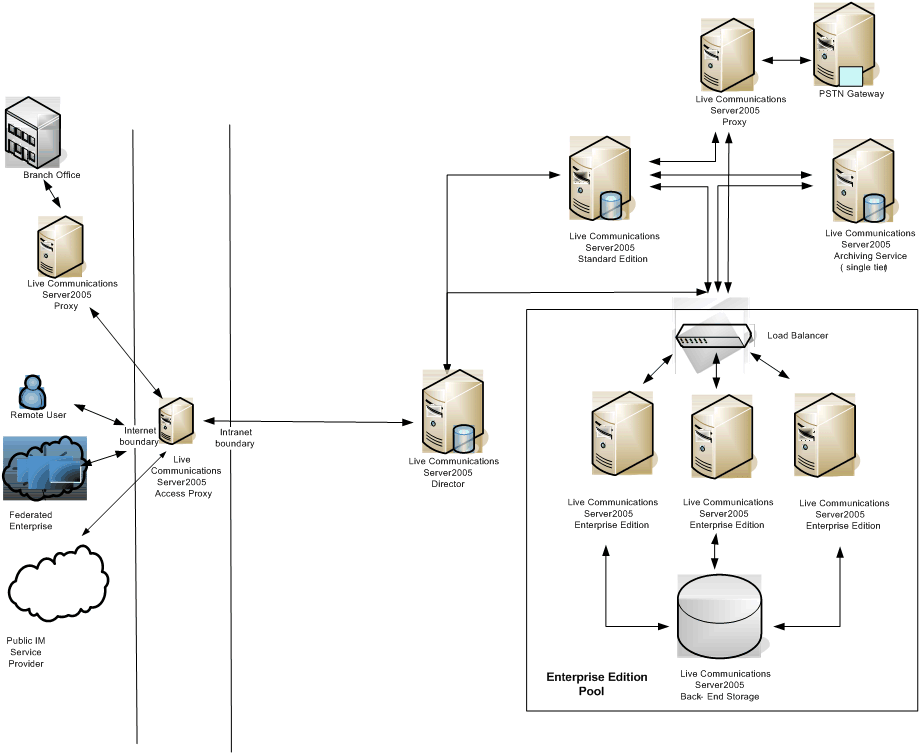


Figure 10. Live Communications Server Enterprise Edition infrastructure

The final deliverable of the Evaluate and Plan phase is a deployment plan and architectural design for your selected presence infrastructure. For more information about planning for presence using Microsoft technology, see the [Microsoft Office Live Communications Server 2005 with Service Pack 1 Planning Guide](http://www.microsoft.com/technet/prodtechnol/office/livecomm/library/planning/lcspln_1.mspx).

## Phase 4: Deploy

By now the previous phases have derived an inventory of the current practices used for enabling instant messaging and presence, a high-level requirements specification for implementing presence and managed instant messaging, evaluation of presence and instant messaging technology, and a deployment plan for the selected solution. In the Deploy phase, we will implement the selected presence solution. Ancillary to the deployment of new technology, you will also want to examine policies used to manage existing or unmanaged instant messaging; this may include implementing policy restrictions for sending or receiving files, blocking the installation of new applications, or uninstalling unmanaged applications not meeting defined policy guidelines appropriate for your organization.

If you have selected Live Communications Server 2005, you can find detailed deployment planning and execution information in the [Microsoft Office Live Communications Server 2005 with Service Pack 1 Planning Guide](http://www.microsoft.com/technet/prodtechnol/office/livecomm/library/planning/lcspln_5.mspx) on Microsoft TechNet.

## Further Information

For more information, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “presence.”

To see how Microsoft uses Microsoft Office Live Communications Server 2005, go to <http://www.microsoft.com/technet/itshowcase/content/lcs2005twp.mspx>.

## Checkpoint: Secure Communication Mechanism for Presence

|  |  |
| --- | --- |
| X | Requirements |
|  | Assessed any current unmanaged methods used for presence and instant communication. |
|  | Created a requirements specification for presence and instant messaging, aligning to industry or local regulations and policies. |
|  | Evaluated presence and instant technology and created plan to implement your selected solution. |
|  | Implemented presence at minimum through managed instant messaging and optionally through collaboration and e-mail infrastructure. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Secure Communication Mechanism for Presence capabilities of the Infrastructure Optimization Model.

Go to the [next Self-Assessment question](#_Requirement:_Security_and_5).

# Requirement: Active Directory and IAS/RADIUS for Wireless Network Authentication and Authorization

## Audience

You should read this section if you have not deployed a secure wireless network using Active Directory and IAS/RADIUS for authentication and authorization.

## Overview

Wireless technology releases us from copper wires. A user can have a notebook computer, PDA, Pocket PC, Tablet PC, or just a cell phone and stay online anywhere a wireless signal is available. The basic theory behind wireless technology is that signals can be carried by electromagnetic waves that are then transmitted to a signal receiver. But to make two wireless devices understand each other, we need protocols for communication. Remote Authentication Dial-In User Service (RADIUS) is a client/server protocol where RADIUS clients send authentication and accounting requests to a RADIUS server. The RADIUS server checks the remote access authentication credentials on the user accounts and logs remote access accounting events.

Internet Authentication Service (IAS) in Windows Server 2003 or Network Policy Server (NPS) in the future with Windows Server Code Name “Longhorn” are Microsoft implementations of a RADIUS server and proxy. As a RADIUS server, IAS performs centralized connection authentication, authorization, and accounting for many types of network access including wireless, authenticating switch, and remote access dial-up and virtual private network (VPN) connections. As a RADIUS proxy, IAS forwards authentication and accounting messages to other RADIUS servers. RADIUS is an Internet Engineering Task Force (IETF) standard.

## Phase 1: Assess

You read in previous sections of this guide and in the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* about the importance of authenticating users for access to your IT environment. To move to the Rationalized level, you need to take the next step by expanding authentication and authorization to users independently of their method of accessing your network.

The Assess phase will again take an inventory of any existing wireless infrastructure in place in your organization. Many organizations already have wireless networking capabilities in place and there are three common types of wireless networking technologies:

* Wireless local area networks (WLAN)
* Wireless personal area networks (WPAN)
* Wireless wide area networks (WWAN)

The following sections explain each of these network types and available wireless technologies; the Core Infrastructure Optimization Model focuses on WLAN as the only type of wireless network where your organization can actively control user or object authentication.

### Wireless Local Area Networks (WLAN)

WLAN technologies enable wireless network connections within a private area, such as a company office or building, or in a public area such as an airport or shop. WLANs are generally used to supplement an existing wired LAN environment, providing an extra level of flexibility for the WLAN users, usually at the cost of network speed and connection reliability.

### Wireless Personal Area Networks (WPAN)

WPAN technologies are designed to allow users to establish as needed wireless communications between personal devices such as PDAs, cellular phones, or laptops. Generally these devices are designed to communicate in an area of a few meters, an area referred to as a personal operating space (POS).

### Wireless Wide Area Networks (WWAN)

WWAN technologies are designed to enable wireless connections over public or private networks that are distributed over large geographical areas, such as cities or countries.

The result of the Assess phase will be documentation of existing WLAN topologies in use at your organization. This topology will be used in the Evaluate and Plan phase while planning for ways to optimize secured user authentication.

## Phase 2: Identify

The Identify phase concentrates primarily on identifying a secure means of authenticating WLAN-connected devices in an effort to mirror the level of security used in your wired LAN infrastructure. This section introduces the following technologies and protocols used to provide a secure wireless networking infrastructure:

* Wireless authentication using IEEE 802.11
* Remote Authentication Dial-In User Service (RADIUS)
* Extensible Authentication Protocol (EAP)
* Internet Authentication Service (IAS)
* Certificates

For detailed technical guidance about wireless protocols and authentication, see the [Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx).

### Wireless Authentication Using IEEE 802.11

The Institute of Electrical and Electronics Engineers, Inc. (IEEE) 802.11 is an industry standard for a shared access WLAN that defines the Physical layer and media access control (MAC) sublayer for wireless communications. The original IEEE 802.11 standard defined the following types of authentication, which are described in the following sections.

#### Open System Authentication

Open system authentication does not provide authentication, only identification using the wireless adapter's MAC address. Open system authentication is used when no authentication is required. Open system authentication is the default authentication algorithm that uses the following process:

1. The authentication-initiating wireless client sends an IEEE 802.11 authentication management frame that contains its identity.
2. The receiving wireless node checks the initiating station's identity and sends back an authentication verification frame.

With some wireless APs, you can configure the MAC addresses of allowed wireless clients using a feature known as MAC filtering. However, MAC filtering does not provide any security because the MAC address of a wireless client can be easily determined and spoofed.

#### Shared Key Authentication

Shared key authentication verifies that an authentication-initiating station has knowledge of a shared secret. According to the original 802.11 standard, the shared secret is delivered to the participating wireless clients by means of a secure channel that is independent of IEEE 802.11. In practice, the shared secret is manually configured on the wireless AP and the wireless client.

Shared key authentication uses the following process:

1. The authentication-initiating wireless client sends a frame consisting of an identity assertion and a request for authentication.
2. The authenticating wireless node responds to the authentication-initiating wireless node with challenge text.
3. The authentication-initiating wireless node replies to the authenticating wireless node with the challenge text that is encrypted using WEP and an encryption key that is derived from the shared key authentication secret.
4. The authentication result is positive if the authenticating wireless node determines that the decrypted challenge text matches the challenge text originally sent in the second frame. The authenticating wireless node sends the authentication result.

Because the shared key authentication secret must be manually distributed and typed, this method of authentication does not scale appropriately in large infrastructure network mode (for example, corporate campuses and public places).

### Remote Authentication Dial-In User Service (RADIUS)

RADIUS is a widely deployed protocol enabling centralized authentication, authorization, and accounting for network access. Originally developed for dial-up remote access, RADIUS is now supported by wireless APs, authenticating Ethernet switches, virtual private network (VPN) servers, Digital Subscriber Line (DSL) access servers, and other network access servers.

### Extensible Authentication Protocol (EAP)

The Extensible Authentication Protocol (EAP) was originally created as an extension to Point-to-Point Protocol (PPP) that allows for development of arbitrary network access authentication methods. With PPP authentication protocols such as Challenge-Handshake Authentication Protocol (CHAP), a specific authentication mechanism is chosen during the link establishment phase. During the connection authentication phase, the negotiated authentication protocol is used to validate the connection. The authentication protocol itself is a fixed series of messages sent in a specific order. With EAP, the specific authentication mechanism is not chosen during the link establishment phase of the PPP connection. Instead, each PPP peer negotiates to perform EAP during the connection authentication phase. When the connection authentication phase is reached, the peers negotiate the use of a specific EAP authentication scheme known as an EAP type.

### Internet Authentication Service (IAS)

IAS in Windows Server 2003 and Windows 2000 Server is the Microsoft implementation of a RADIUS server and for Windows Server 2003, the Microsoft implementation of a RADIUS proxy. IAS performs centralized connection authentication, authorization, and accounting for many types of network access, including wireless, authenticating switch, dial-up and virtual private network (VPN) remote access, and router-to-router connections. IAS enables the use of a heterogeneous set of wireless, switch, remote access, or VPN equipment and can be used with the Windows Server 2003 or Windows 2000 Server Routing and Remote Access service.

When an IAS server is a member of an Active Directory-based domain, IAS uses Active Directory as its user account database and is part of a single sign-on solution. The same set of credentials is used for network access control (authenticating and authorizing access to a network) and to log on to an Active Directory-based domain.

### Certificates

Certificates are used to authenticate a wireless client with a wireless access point. Wireless clients running Windows Vista, Windows XP, Windows Server 2003, Windows Server “Longhorn,” and Windows 2000 Server can use certificates to authenticate the computer.

### Identify Phase Summary

The Identify phase for this requirement differs from others in that it contains many of the aspects used for evaluating technology options for wireless networking. This is partly the case because the protocols and standards used are consistent for nearly all wireless networking technologies. An understanding of the standards and protocols is necessary to identify your desired outcome, or requirement specification, for secure wireless authentication. For more information, see the [Wireless Deployment Technology and Component Overview](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx) and [Wireless Networking Security](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wnsec.mspx) guides on Microsoft TechNet.

## Phase 3: Evaluate and Plan

Now that you have identified the technologies and protocols required to wireless network security and developed a high-level requirements specification, the Evaluate and Plan phase will evaluate technologies that can be used to plan and implement your wireless network deployment project.

Assuming that other requirements of the Rationalized level have been fulfilled, many of the components necessary for implementing a secure wireless infrastructure are probably in place, including Windows XP SP2 or newer client computers and Windows 2000 Server or newer servers.

### Windows Server IAS

Windows Server IAS provides the following solutions for organizations that require secure network access:

* Compatibility with RADIUS servers and clients from any vendor that meets the IEEE specifications outlined in RFCs 2865, 2866, and 2869.
* Integration with the Active Directory directory service. IAS allows you to take advantage of Active Directory for user authentication, authorization, and client configuration, thus reducing management costs.
* Use of standards-based strong authentication methods for network access.
* Management of network access that is outsourced to an ISP. IAS allows you to create an agreement between your organization and the ISP in which the ISP can charge a roaming user’s department for that employee’s network usage. In this way, each employee does not need to submit an expense statement or create a roaming account to connect to the corporate network remotely.
* Dynamic key management for wireless access points as a means to increase network security.

Servers running the Internet Authentication Service (IAS) component of the Windows 2000 Server and Windows Server 2003 operating systems perform centralized authentication, authorization, auditing, and accounting for many types of network access, including dial-up, virtual private network (VPN), wireless, and 802.1x authenticating switch access. IAS is the Microsoft implementation of the Remote Authentication Dial-In User Service (RADIUS) protocol.

For more information, see the [Windows Server 2003 Security Guide](http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/sgch00.mspx).

### Active Directory

When you implement your IAS server as a member of an Active Directory domain, IAS uses the Active Directory directory service as its user account database and is part of a single sign-on solution. With single sign-on, users supply account credentials (user name and password or a certificate) only once during the authentication and authorization process; these credentials are then used to log on to an Active Directory domain and for network access control (authenticating and authorizing access to a network).

### Planning a Secure Wireless Network

There are two primary wireless security architectures using Microsoft technologies. The first method uses an IPsec VPN, while the second uses the 802.1x Extensible Authentication Protocol (EAP). The purpose of both is to guarantee the user authentication and authorization and to protect the data's confidentiality and integrity.

#### IPsec VPN Authentication

The basic structure of IPsec VPN is that the wireless clients connect to the open wireless access point (AP) and then authenticate with the IPsec VPN for access to the organization's protected intranet.

#### 802.1x Authentication Using EAP

802.1x with EAP-TLS and machine certificates can be used to authenticate both the wireless clients and the server. It also manages the WEP key by periodically and automatically sending a new key, thereby avoiding some of the known WEP key vulnerabilities. The data confidentiality will be protected by these dynamic WEP keys.

When creating your plan for implementation, you can use either method. For more information, see the [Wireless Networking Security](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wnsec.mspx) guides on Microsoft TechNet.

Also see [Securing Wireless LANs with PEAP and Passwords](http://www.microsoft.com/technet/security/guidance/cryptographyetc/peap_0.mspx) and [Securing Wireless LANs with Certificate Services](http://www.microsoft.com/technet/security/prodtech/windowsserver2003/pkiwire/swlan.mspx?mfr=true) guides on Microsoft TechNet.

## Phase 4: Deploy

The final step in the process is to deploy protected wireless access in your organization. If you have selected the 802.1x authentication method using Windows technologies, detailed step-by-step deployment guidance can be found in the [Deployment of Protected 802.11 Networks Using Microsoft Windows Guide](http://www.microsoft.com/technet/prodtechnol/winxppro/deploy/ed80211.mspx).

## Further Information

For more information on Active Directory and IAS/RADIUS, go to the following Web sites:

* <http://technet2.microsoft.com/WindowsServer/en/library/55f10dbe-c5d8-497e-8bd1-f0d6d8019ee41033.mspx?mfr=true>
* <http://www.microsoft.com/technet/security/midsizebusiness/topics/serversecurity/wirelessaccessconfig.mspx>
* <http://www.microsoft.com/technet/isa/2006/authentication.mspx>

You can also visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “IAS” or “RADIUS.”

To see how Microsoft uses IAS, go to <http://www.microsoft.com/technet/itshowcase/content/secnetwkperim.mspx>.

## Checkpoint: Active Directory and IAS/RADIUS for Wireless Network Authentication and Authorization

|  |  |
| --- | --- |
| X | Requirements |
|  | Identified current wireless access and related topologies. |
|  | Evaluated wireless technologies, protocols, and standards. |
|  | Developed and implemented plans for secure wireless authentication infrastructure. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Active Directory and IAS/RADIUS for Wireless Authentication and Authorization capabilities of the Core Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources in the [Wireless Resources for Windows XP on Microsoft TechNet](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wireless.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Security_and_6).

# Requirement: Centrally Managed Certificate Services

## Audience

You should read this section if you do not have a centrally managed Certificate Services infrastructure or Public Key Infrastructure (PKI).

## Overview

Computer networks are no longer closed systems where the mere presence of a user can serve as a sufficient proof of identity. In this age of information interconnection, the network of an organization may consist of intranets, Internet sites, and extranets, all of which are susceptible to intrusion by individuals with malicious intent seeking a variety of data files, from e-mail messages to e-commerce transactions. To mitigate the risks incurred by this susceptibility, mechanisms for establishing and sustaining a user's identity are required. A centrally managed, electronic identity for users can provide the following:

* **Accessibility of information.** Information assets need to be accessible to authorized users and protected from unauthorized access or modification. Passwords can help, but users who have several passwords for accessing different secure systems may choose passwords that are easy to remember and consequently easy to decipher.
* **Non-repudiation of identity.** Information needs to be sent from one user to another with the confidence that the sender of the information is valid. It is also necessary to provide reasonable confidence that the information has not been changed en route.
* **Privacy of information.** Users should be able to send information to other users or to access a computer system with confidence that the information cannot be accessed or be made available to others. It should be possible for the user or system to define who can access the information. Privacy is of particular importance when information is transmitted over the public Internet.

These requirements deal with electronic information assets and have a direct impact on most organizations. Any mechanism that is implemented to deal with these requirements must be both manageable and secure. A public key infrastructure (PKI) is an appropriate technology to fulfill these requirements with the use of digital certificates. PKI enables the exchange of digital certificates between authenticated entities and trusted resources. Certificates in a PKI are used to secure data and manage the identification credentials of resources within and outside the organization. Clearly, PKI itself needs to be trusted; therefore, it is managed by a pre-qualified organization or part of such organization. Such an organization can be called a certification authority (CA), but usually just the computer that runs the certificate software is called a CA. Whether the CA refers to an organization or to the software that supports certification, the CA is responsible for establishing and vouching for the identity of certificate holders. It may also revoke certificates if they should no longer be considered valid and publish certificate revocation lists (CRLs) for use by certificate verifiers to determine the validity of a certificate.

This guide uses best practices as documented by the [Windows Server System Reference Architecture Certificate Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/certificateservices/default.mspx) guides.

## Phase 1: Assess

The Assess phase looks at the current state of the network environment. This Assess phase is identical to the Assess phase in the requirement for [Secured and Guaranteed Communication Verification Between Servers](#_Requirement:_Secured_and) at the Rationalized level. The process of obtaining and maintaining a reliable record of an organization's computers, software, and network devices is a classic IT challenge. Information about the following items is required to define the current state:

* Network discovery
* Documentation of network segmentation
* Network infrastructure devices
* Analysis of current network traffic model
* Active Directory
* Host discovery
* Host data requirements

For detailed information on how to gather this information, read the [Server and Domain Isolation Using IPsec and Group Policy Guide Chapter 3: Determining the Current State of Your IT Infrastructure](http://www.microsoft.com/technet/security/guidance/architectureanddesign/ipsec/ipsecch3.mspx). This guide discusses the requirements for each item and how to collect information via automated discovery using [SMS 2003](http://go.microsoft.com/fwlink/?LinkId=69780) or similar products as well as manual discovery options.

## Phase 2: Identify

The Identify phase defines the high-level need for establishing a centralized public key infrastructure. When an organization decides to implement a PKI, the business problem should be identified before the design phase starts. The design phase begins with identifying the considerations for people, processes, and technology. The questions that drive the PKI service requirement include the following:

**People-related questions:**

* How do people handle their certificates?
* Who is going to manage the certificates?
* How does a PKI affect a user’s working experience?
* What is the size of the organization?

**Process-related questions:**

* Should the PKI be part of the organization's IT infrastructure or should the certificates be bought from an outside source?
* Are certificates also used for external transactions?
* What process is applied to enroll certificates?
* How are trusts established and verified between the organization and related entities?
* At what intervals should a trust be verified?
* What constraints have an impact on the validity of certificates?
* How urgent is the revocation of associated certificates once a trust is canceled?

**Technology-related questions:**

* What are the types of entities that require certificates, and for what purposes?
* For what purposes is a directory service beneficial?
* What information needs to be included as part of the certificates?
* Which applications are PKI-enabled?
* How complex should a public/private key be, and can PKI-enabled applications support this complexity?

Before the first CA server is installed in an organization, a complete PKI service design study must exist that covers people, processes, and technology. In the long run, extending a poorly implemented PKI is more difficult and costlier to manage than spending time up front to plan for an extensible PKI. For more information about identifying the high-level requirements of the PKI, see the [WSSRA Blueprint for Enterprise Design for Certificate Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/CertificateServices/CrtSevcBP_2.mspx).

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, we will examine PKI and plan the necessary steps for deploying the infrastructure.

### What Is PKI?

Many of the technologies needed to implement a secure network require PKI, which enables the exchange of digital certificates between authenticated entities and trusted resources. Certificates in a PKI are used to secure data and manage the identification credentials of resources within and outside the organization. When a PKI is in place, any permitted subject is allowed to request certificates from a certificate enrollment service that is managed by the CA. The CA determines the validity of the certificate requester and issues a valid certificate in response to the request. The certificate holder can use the certificate until it expires or until it is revoked; the trustworthiness of a certificate depends on the quality of trust between a certificate requester and the issuing CA. Two user certificates issued by two different CAs will, by default, have no trusted status between each other. A common trust between the issuing CAs is required to ensure that the certificates can be mutually trusted.

PKI-enabled clients use certificates to determine the level of trust for a given resource. To ensure this, a PKI needs a verification mechanism to check a certificate’s validity. The Windows Server 2003 PKI provides CRLs as a verification mechanism, and clients are technically capable of retrieving a CRL through a number of protocols. Depending on the client capabilities and the network infrastructure, use of one protocol might be preferred over the others; examples of such protocols include:

* **HTTP and Secure HTTP (HTTPS).** HTTP and HTTPS are used when CRLs are published with a Web server. These protocols are commonly used to make CRLs accessible to entities outside the organization's network.
* **LDAP.** Accessing a CRL through LDAP from a directory service requires more bandwidth than retrieving the same CRL through HTTP because LDAP, by default, requires authentication. Even if anonymous access is used to retrieve the CRL, LDAP would send an anonymous authentication header. If a CRL needs to be available internally and externally, it can be difficult to provide directory access to all clients through LDAP.

### PKI Architecture

The architecture of a PKI involves implementing various interdependent technologies and processes to make it possible to issue, validate, renew, and revoke certificates. These technologies include:

* One or more servers running certificate services that provide certificate enrollment, revocation, and other certificate management services.
* Active Directory directory service or another directory service that provides account management, policy distribution, and certificate publication services.
* Domain controllers that can authenticate end users and computers when they request certificates.
* Domain client computers and users who request, receive, and use certificates for specific purposes. Although certificates can also be used by services and by non-domain clients, in most Windows PKI environments, domain users and computers are the primary recipients and users of certificates. In some cases, the domain client can be a subordinate CA that requests and receives a certificate authorizing it to issue certificates of its own.

The following figure illustrates the architecture of PKI technologies.

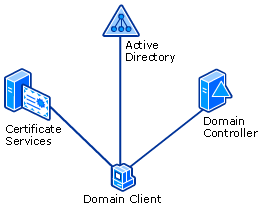


Figure 11. PKI technologies architecture

This type of PKI implementation gives you centralized control over your certificate services.

### Planning for CA Infrastructure and PKI Implementation

The options for a CA infrastructure depend on the security and certificate requirements of an organization, the purpose of the PKI, and the requirements of applications, users, and computers.

As described earlier, certificate requirements have a direct impact on your PKI design. Logical design of the PKI can be done once the PKI service has been defined. See the [WSSRA Blueprint for Enterprise Design for Certificate Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/CertificateServices/CrtSevcBP_2.mspx) for detailed technical guidance for planning your organization’s public key infrastructure.

## Phase 4: Deploy

After your public key design has been validated and refined by lab testing and pilot programs, you can deploy the PKI in your production environment. A disciplined approach to deploying a PKI is essential for establishing the security of the applications that you are enabling. The following figure shows the high-level CA infrastructure and PKI deployment processes.

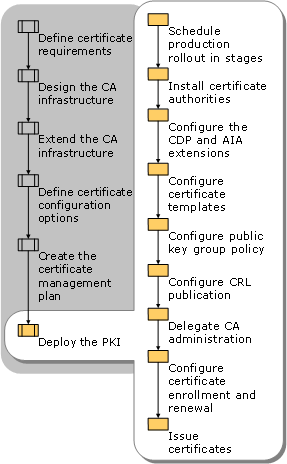


Figure 12. High-level CA infrastructure and PKI deployment processes

For detailed technical information on CA infrastructure and PKI deployment, see:

* [Windows Server 2003 Technical Library: Designing a Public Key Infrastructure](http://technet2.microsoft.com/WindowsServer/en/library/b1ee9920-d7ef-4ce5-b63c-3661c72e0f0b1033.mspx)
* [Windows Server 2003 Technical Library: Deploying the PKI](http://technet2.microsoft.com/WindowsServer/en/library/169a7f14-896f-4b8c-a29f-d8116709a0c01033.mspx)

## Further Information

For more information, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “PKI.”

To see how Microsoft deploys PKI, go to <http://www.microsoft.com/technet/itshowcase/content/deppkiin.mspx>.

## Checkpoint: Centrally Managed Certificate Services

|  |  |
| --- | --- |
| X | Requirements |
|  | Performed a network discovery to inventory all components. |
|  | Identified people, process, and technology design considerations for the certification authority and public key infrastructure. |
|  | Created a detailed deployment plan to enable the PKI. |
|  | Implemented PKI deployment plan. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Centrally Managed Certificate Services capabilities of the Core Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for certificate services.

Go to the [next Self-Assessment question](#_Requirement:_Security_and_7).

# Requirement: Proactively Managed Bandwidth to Branch Offices

## Audience

You should read this section if you do not proactively manage bandwidth to branch offices.

## Overview

When you must provide secure, safe, and efficient communication between your organization’s headquarters and branch offices, you face the issue of limited bandwidth over your wide area network (WAN). There are several things you can do to make the most efficient use of the bandwidth. The design of your physical network infrastructure has a significant impact on other services and components in your branch and hub site infrastructures. The performance and availability of the network determine whether a service can appropriately support user requirements for accessing services over a WAN.

This guide is based on published guidance in the [Branch Office Infrastructure Solution for Microsoft Windows Server 2003 Release 2 (BOIS R2)](http://www.microsoft.com/technet/solutionaccelerators/branch/default.mspx).

## Phase 1: Assess

The following sections discuss the activities you should conduct during the Assess phase.

### Documenting Network Design

The first step in determining how to optimize WAN bandwidth in your organization is to document your organization’s current network design for branch offices. There are two primary branch office network designs: single-hub and multi-hub.

#### Single-Hub Network

In a single-hub network, the hub site connects directly to multiple remote sites. This is a common WAN structure for organizations that have multiple branch offices, but the branch offices have almost identical business functions and operate within the borders of a single country or smaller region. The following figure shows a sample network structure with one hub site.

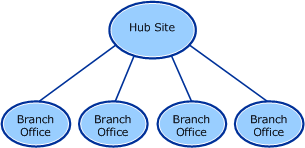


Figure 13. Single-hub network

#### Multi-Hub Network

The multi-hub network generally provides at least three tiers of network connections. This is a common structure for larger or international organizations that have many branch offices with diverse business functions. This WAN structure commonly has one central hub site for corporate headquarters and one hub site per geographic region. The following figure shows a sample network structure with one central hub site and two regional hub sites.

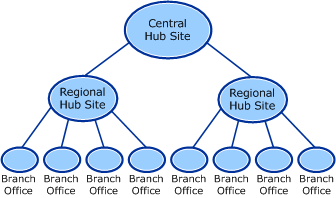


Figure 14. Multi-hub network

The multi-hub network may be further extended if branch offices are connected to other branch offices. In this case, it is important to determine the services to be available in second-tier sites. Options for the second-tier sites include the following:

* Have the same set of services available locally as the first-tier branch office.
* Have more services available locally (because of insufficient network availability, capacity, or performance).
* Have fewer services available locally and rely on the services provided by the hub site.

The first step of the Assess phase is to document your organization’s network design for your branch and hub infrastructure.

### Documenting WAN Links

The next step in the Assess phase is to document the WAN links between all of your sites. The network link connecting the branch office to the hub site is a critical component of any WAN. The WAN link can significantly affect the availability of any services requiring access over the WAN. As part of the discovery process, you should determine the following information:

* **Link type**. This is a primary determinant of network speed, support for network loads, and network availability. Link type includes whether the connection is persistent (such as a leased line) or on-demand (such as dial-up and ISDN), as well as the protocols that it uses (such as virtual private networking or VPN, Frame Relay, or satellite).
* **Link bandwidth**. This is the theoretical maximum speed of the link, but the real speed is limited by network latency.
* **Link latency**. This is the time that it takes a network packet to get from one place to another, which constrains the minimum time (amount of delay) it requires for a transaction (round trip).
* **Link capacity**. This is the theoretical amount of aggregate data that can be pushed through a network link. It is closely tied to link speed.
* **Link utilization**. This is expressed as a percentage of total capacity for the link. Utilization includes all network traffic, including the background transactions required to monitor and manage the network and services, other individual services and applications that use the network, and specific functions that depend on the network (such as security cameras/systems and VoIP).

### Network Segmentation in the Branch Office

The last stage is assessing network segmentation for the branch office and what is required to most appropriately support the services in the new solution.

The internal network in the branch office has traditionally been a single segment network, also known as a flat network. This type of network provides a simple and inexpensive infrastructure with a simple IP plan. If your organization’s branch offices incorporate single or multiple segment networks, these should be documented as part of the assessment.

### Other Network Design Considerations

In addition to the network link, each branch office also requires a network infrastructure that supports all users in the branch office and their internal connectivity requirements. Additional design considerations related to the branch infrastructure and other network components include the following:

* Location of centralized services
* Local Internet access
* Security impacts
* Routing limitations
* Network Address Translation (NAT)

### Assessment Summary

The outcome of this step should produce a detailed spreadsheet or topology diagram listing how all of these items correlate to the network design documented in the first step. For more information and other assessment considerations, see [Physical Design in the BOIS R2 guide](http://www.microsoft.com/technet/solutionaccelerators/branch/boisv2_13.mspx).

## Phase 2: Identify

The goal of the Identify phase is to determine the level of performance appropriate for your organization’s needs. In most cases increasing performance will lead to increasing costs. In this phase it is important to weigh the costs and benefits of each performance level.

The diverse type and characteristics of WANs make it impossible to give specific recommendations about which WAN connections are most appropriate for your organization. However, based on customer data collected by various groups, it is possible to generalize three network link scenarios: high, medium, and low performance. The following list describes the characteristics of each of these performance scenarios and the potential applications for each:

* **High performance**. Satellite branch offices typically require high performance links, (at least 1.544 or 2 megabits per second or Mbps, depending on location), low latency, and high availability. These are typically found in North America and within country borders of many Western European and other countries. This type of network link may enable organizations to centralize more services into the hub site than the other scenarios simply because the reduction in management cost by moving services centrally can outweigh the cost of providing sufficient availability. Also, the capacity and latency can be good enough that they should not negatively affect end-user productivity. In some cases, productivity may actually improve because of application. For instance, applications that access a back-end store (such as a database or mainframe computer) in a hub site might benefit by being moved to application farms in a central site and by using Terminal Services to access them. The reason for this is that the most intensive transactions do not have to occur over the WAN, and the high-capacity WAN supports the level of performance that users require for access to the application.
* **Medium performance**. Accelerated branch offices can typically use medium performance links (128–512 kilobits per second or Kbps), medium latency, and good availability. These scenarios are typically found in geographic locations that do not have the more advanced telecommunication infrastructures or in situations that require crossing significant geographic boundaries. The link might support centralization of services with low bandwidth requirements (such as DNS and Active Directory), if they do not have configurations or other restrictions that prevent centralization. However, the availability of the network link might not be sufficient to ensure that the services left in the branch office (such as file and print services) can access any centralized services upon which they depend for name resolution, authentication, and authorization. Also, the latency of this link might not provide an acceptable user experience when using Terminal Services to access centralized applications.
* **Low performance**. Autonomous branch offices can usually function with lower performance links (such as those less than 128 Kbps) and high latency and are more tolerant of link unreliability. This scenario is typically found in areas of the world where the telecommunications industry is significantly under-developed or the cost of actually obtaining a higher performing and more available network link is cost prohibitive (such as when connecting a single branch office in a very remote location). Use of this type of link is not conducive to the centralization of services. But it simplifies the branch office design because all services that support the business-critical branch office functions and the services upon which they depend must be located locally in the branch office.

The result of the Identify phase should be a detailed analysis and recommendation of the desired performance outcomes for each connection, thereby determining how each branch office is classified: satellite, accelerated, or autonomous.

## Phase 3: Evaluate and Plan

Until now, you have been documenting your network topology and desired performance needs for your branch office infrastructure. In the Evaluate and Plan phase, you will evaluate the impacts of centralizing versus localizing services and create a plan for managing your WAN links to meet your performance requirements.

### Evaluating the Physical Server Design

Branch office infrastructure design is generally focused on centralizing as many services as possible. Although a long-term goal might be to centralize all services, this is seldom feasible for a short-term solution. The reason for this is that it can be cost-prohibitive to provide connectivity between the client computer in the branch office and the service in the hub site that has appropriate availability, capacity, and latency. If the state of current technologies does not support centralization of specific services, the intent of streamlining the branch design is usually to consolidate all services remaining in the branch office on a single server. This can also be challenging but is achievable in certain instances.

The types of design considerations that are not specific to a single service and that should be applied to all services include the following:

* The design options available for streamlining branch office infrastructures.
* Branch service placement considerations, including the general implications of service placement on people and processes, as well as on the business itself.
* Other design considerations, especially those related to users and business functionality, which are not specific to service placement.

#### Design Options for Branch Office Infrastructures

Defining branch office infrastructures requires analyzing the options for and implications of deploying services centrally and locally. The two basic decisions that you must make for each branch require evaluation of many design options.

##### Service Centralization Options

The primary options available for centralization of services include running the service:

* Only in the branch office (with no failover).
* In the branch office with failover to the hub site if it has replication capabilities.
* Only in the hub site.

##### Branch Server Design Options

You can still streamline services that cannot be centralized by service consolidation on one or more branch servers. The branch server design should focus on how to optimize the use of hardware, software, and support (including the use of personnel resources) in each branch office.

The [Solution Accelerator for Consolidating and Migrating LOB Applications](http://go.microsoft.com/fwlink/?LinkId=47191) and the [Mixed Workload Consolidation Guide](http://go.microsoft.com/fwlink/?LinkId=46571) provide detailed guidance for determining which applications can be consolidated. The [Solution Accelerator for Consolidating and Migrating LOB Applications](http://go.microsoft.com/fwlink/?LinkId=47191) also provides guidance for identifying appropriate solutions for applications that are not good candidates for consolidation.

The following list summarizes the primary options for running applications at branch office sites:

* Single server consolidation
* Service consolidation
* Virtualized consolidation
* Dedicated server

The option that you choose for each service determines the number of branch servers required.

#### Branch Service Placement Considerations

Each organization has priorities that dictate which requirements are most significant and, thus, which ones will have the most impact on the design of the branch office infrastructure solution. As part of your earlier analysis efforts during the Envisioning phase of your project, you should have identified technical, business, and other requirements and limitations that affect the placement of services.

You will need this information to effectively evaluate the options and trade-offs for each branch service—both the general design considerations and the service-specific design considerations that the following list outlines:

* IT organization
* Political considerations
* Legal and regulatory considerations
* Security
* Availability and reliability, including:
* Centralization of services
* Consolidation and co-hosting services on a branch server
* Non-redundant servers in the branch office
* Branch service redundancy
* Single server for local services, with local redundancy and Windows clustering for services
* Backup and recovery
* Performance and capacity
* Scalability
* Cost

### Planning for Branch Office Services

BOIS R2 introduced a new design technique that you can use to provide a common and repeatable approach to infrastructure service design in an organization, whether for branch offices or other IT services. This technique uses service design reference (SDR) diagrams and three fundamental design elements to illustrate the design process for each service. These elements are:

* Design stages
* Design considerations
* Design options

The following figure shows a generic version of a service design reference that is used to illustrate the elements of this design approach.

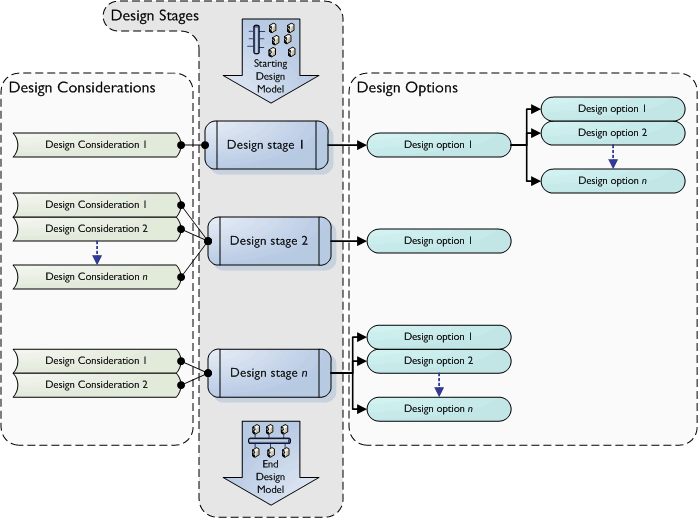


Figure 15. Generic version of a service design reference

At each design stage, you should use the considerations and options to determine whether the input design will meet the requirements of the new design and whether the model can be modified to match the new requirements as needed.

Detailed planning is required for the core branch office service to ensure that WAN bandwidth usage is optimized. These services are referred to as *core services* because they provide the basic infrastructure for a branch office environment that can then be enhanced or extended to increase the features of a solution. These core services are:

* Directory Service
* Network Addressing and Name Resolution Services
* File Services
* Print Services
* Core Client Services
* Core Management Services

See the [Core Branch Service Design in BOIS R2](http://www.microsoft.com/technet/solutionaccelerators/branch/boisv2_18.mspx) for detailed information about designing for branch office core services.

### Distributed File System

The Distributed File System (DFS) technologies in Windows Server 2003 R2 offer WAN-friendly replication as well as simplified, fault-tolerant access to geographically dispersed files. The two technologies in DFS are as follows:

* **DFS replication**. New state-based, multimaster replication engine that is optimized for WAN environments. DFS Replication supports replication scheduling, bandwidth throttling, and a new byte-level compression algorithm known as remote differential compression (RDC).
* **DFS namespaces**. Technology that helps administrators group shared folders located on different servers and present them to users as a virtual tree of folders known as a namespace. DFS Namespaces was formerly known as Distributed File System in Windows 2000 Server and Windows Server 2003.

### Evaluating and Planning Summary

There is no single step or recommendation for optimizing WAN bandwidth in every organization. Each organization has unique considerations when managing their WAN. As a result of the Evaluate and Plan phase, the goal is to identify where opportunities exist to consolidate services and have a better understanding of your current network topology so that WAN bandwidth can be proactively managed.

## Phase 4: Deploy

Once you have identified the appropriate architectures and balance of centralized versus localized services for your branch offices in order to optimize WAN link constraints, the Deploy phase will implement the recommendations resulting from your branch office planning and architecture. Depending on the recommendations made, the Deploy Phase may, for example, lead to further centralization of services and, with those changes, WAN links will be adjusted appropriately. As part of the deployment process, it can be written as a standard policy to reexamine WAN link requirements and branch office infrastructure at appropriate intervals or corresponding with preset data, performance, or staffing thresholds.

## Further Information

For more information, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “bandwidth management.”

To see how Microsoft manages WAN bandwidth, go to <https://www.microsoft.com/technet/itshowcase/content/optbwcs.mspx>.

## Checkpoint: Proactively Managed Bandwidth to Branch Offices

|  |  |
| --- | --- |
| X | Requirements |
|  | Identified and documented branch office topology. |
|  | Created requirement specification based on the needs of all branch office types. |
|  | Created a plan and architecture for branch office service consolidation and identified performance thresholds for reexamination of branch office WAN requirements. |
|  | Implemented plan to optimize branch office services against WAN link limitations. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Proactively Managed Bandwidth to Branch Offices capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for managing bandwidth.

Go to the [next Self-Assessment question](#_Requirement:_Data_Protection).

Capability: Data Protection and Recovery

# Introduction

Data Protection and Recovery is the fourth Core Infrastructure Optimization capability. The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Data Protection and Recovery.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  User and application data management is decentralized, increasing operations costs  Not regulatory compliant, which could lead to financial penalties  **IT Challenges**  Application data management is segmented. The unreliability of tape-based backups and slow data transfers are still an issue.  Traditional data backup methods provide inadequate infrastructure protection | **Projects**  Implemented centrally managed data backup for branch offices  Implement full-scale deployment of data protection tools  Implement a NAS/SAN-centralized DRP or business continuity and disaster recovery solution for all servers to meet required SLAs | **Business Benefits**  Streamlined support processes through consolidated data management  Closer to implementing regulatory compliance  Improved productivity due to better performance of backup services that stabilize the environment  Backup ”windows” more efficient, retaining the streamlined support process and minimizing the impact to the business  **IT Benefits**  Established SLAs between business and IT  Reduced operations costs through centralized mission-critical user and application data  Spend less time on data backup and recovery operations |

The Rationalized Level in the Infrastructure Optimization Model addresses key areas of networking and security components, including:

* Centrally managed data backup for branch offices.
* Backup, restore, and defined recovery times for servers.

# Requirement: Centrally Managed Data Backup for Branch Offices

## Audience

You should read this section if you do not centrally manage data backup for your branch offices.

## Overview

Organizations with branch offices need the ability to protect and restore data centrally so that employees in the field can concentrate on their core functions. Managing data backup at individual sites poses numerous problems. As personnel, hardware, and software changes, you would need to constantly retrain staff at remote locations.

Which backup and recovery solution is most appropriate for branch services depends on the location of the services, the facilities available at the branch location, and the nature of the data stored. The need for business continuity and the number and type of decisions required to define appropriate backup and recovery solutions can affect where you locate each branch service. The backup and recovery of services and data over the WAN can introduce significant amounts of traffic—the decision to centralize must take such impacts into account. Co-locating services can introduce additional challenges.

When you have centralized backup of branch offices, you can provide better service in several ways. Your backup and restore software should provide the following capabilities:

* **No user intervention.** Local users do not need to remember to rotate the data backup tapes into tape backup hardware.
* **Automated monitoring.** You can verify the success and health of the backed-up production servers. The software should give you just-in-time alerts about issues that you need to fix.
* **Faster and more reliable restorations.** The software must provide rapid and reliable recovery of data lost because of user error or server hardware failure. End-user recovery enables users to independently recover their own data.
* **Verification of backups.** You can easily verify the success of a backup.
* **Monitored backup process.** You can verify the success and health of the backup process.

## Phase 1: Assess

While there are two basic options for the branch office backup approaches, local and central, the reality is that most organizations will have adopted a hybrid approach. The Assess phase will examine the current backup and recovery methods for branch office data. The result of the Assess phase should be a process mapping of the backup and restore functions of both central data repositories and local branch office data repositories.

In the [Backup, Restore, and Defined Recovery Times for Servers requirement](#_Requirement:_Backup,_Restore,) in this guide, we describe the need for backup and recovery of all servers with attached SLAs. For centralized data repositories, these concepts apply to backup of branch office-generated data. For local data repositories, the requirement of [Proactively Managed Bandwidth to Branch Offices](#_Requirement:_Proactively_Managed) will also apply to the backup and recovery procedures selected as a result of this exercise. Often given the constraints of WAN links, the appropriate level of data backup moving over the network to central sites will vary depending on the organization and geographical topology. The purpose of the Assess phase is really to identify insufficient or as needed local backup routines.

## Phase 2: Identify

During the Identify phase, it is often best to begin with a thorough examination of regulations, local laws, and industry requirements as they pertain to data backup and archiving. After identifying compliance issues associated with data backup, identify the WAN-link limitations or constraints that need to be dealt with when planning for how your organization will centrally manage branch office backup. The final deliverable using these and any additional inputs will be to create a requirements specification for the branch office backup service.

## Phase 3: Evaluate and Plan

Operationally, to minimize the need to perform local backups of branch servers, you should consider centralizing as many of the core branch infrastructure services as possible or use backup and recovery methods that enable the central storage of backed-up data. In the Evaluate and Plan phase, consider the technologies available to you to enable a centralized backup and also consider the local tasks that can be managed by establishing policies or guidelines for data retention. The combination of how backups are performed over the network and which local backups are made on-site and how they are securely archived will help formulate a plan to centrally control backup and recovery operations at your branch offices.

### Data Backup and Restore Considerations

When you select and implement a backup and restore solution for your branch offices, you need to address the following:

* Data and system availability
* Network considerations
* Verification

#### Data and System Availability

Backup functions should have a minimum impact on end users’ access to data. Backups also should not affect system performance. Restoring data should be efficient to minimize the time users are unproductive because of data loss.

#### Network Considerations

Your available WAN bandwidth can be a determining factor in the following areas:

* Frequency of backups
* Timing of backups
* Guaranteed restore times
* Type of backup—full or incremental

#### Verification

Your backup software should allow you to verify the success of data transfer for both backup and restore. You should also be able to monitor, track, and record all operations so that you can measure the effectiveness of your backup and restore functions.

For more information on backup and recovery, visit <https://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/BackupandRecoveryServices/igbrbp_2.mspx>.

### Data Replication

Another approach to data backup is data replication. Microsoft System Center Data Protection Manager (DPM) is a disk-based backup solution for file servers that uses the Volume Shadow Copy Service (VSS) to provide access to multiple point-in-time snapshots of protected data. NSI Software, Inc., Double-Take provides real-time data protection and replication. It provides disaster recovery and high availability for the data, thus enhancing the value of DPM to customers.

The ways that you can centralize the management of data protection and recovery by using Data Protection Manager 2006 for backup are described in the following sections.

#### Centralize Branch Office Backups

The most common method for protecting the data on file servers in remote physical locations is for the branch office staff to back up data to removable media such as tape, and then transport the media to an off-site storage facility. DPM makes it feasible to back up the data from remote file servers to disks in the central data center, where the data can then be more efficiently and reliably backed up to tape by central IT staff. Because the DPM server in the data center provides short-term, disk-based recovery, branch offices gain rapid, reliable short-term recovery at a lower cost.

#### Centrally Manage Shadow Copies and End-User Recoveries

By storing the shadow copies used for end-user recovery on the DPM server rather than on individual file servers, you can centralize the management of end-user recovery for multiple file servers.

#### Centrally Monitor DPM Servers and Protected File Servers

As part of your data management strategy, you can use the Data Protection Manager 2006 Management Pack for Operations Manager 2005 (MOM) to centrally monitor data protection, state, health, and performance of multiple DPM servers, and the file servers that they protect, in MOM. From the MOM Operator console, an administrator can monitor DPM and network infrastructure simultaneously, analyzing issues with data protection in the context of other factors in system and network performance. The administrator also can monitor other mission-critical applications, such as Microsoft SQL Server. For information about downloading the DPM Management Pack, see <http://go.microsoft.com/fwlink/?LinkId=47215> .

For more information on data replication, visit <http://www.microsoft.com/technet/prodtechnol/dpm/deploy/dpmnsidoubletake.mspx>.

### Local Backup Policies and Guidelines

Based on the model selected, regulations, and geographic distribution of your organization, you may opt for a hybrid plan for backup and recovery services. Centralized data repositories will continue per the backup and recovery requirement in this guide, and a centralized technology such as Data Protection Manager may take on items appropriate for network-based backup. The nature of this data backup must meet constraints posed by WAN links. If, for example, you have a branch office location in a remote location where less than 128 Kbps is available, your central backup strategy may need to rely upon local backup and storage routines and manual processes.

### Evaluating and Planning Summary

The final outcome of the Evaluate and Plan phase will be a deployable plan consisting of the backup and recovery design for your organization’s branch office-generated data. This plan will be used in the Deploy phase to help implement or broaden the coverage of a technology such as DPM, or it may be used to implement process controls for localized branch office backup and recovery services with defined service levels in accordance with those outlined in the requirement for [Backup, Restore, and Defined Recovery Times for Servers](#_Requirement:_Backup,_Restore,).

For organizations with as needed backup and recovery in branch locations, the [Windows Server System Reference Architecture implementation guides for Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx) can help derive plans for solidifying local operations. Additionally, the [Microsoft Operations Framework Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx) guidance provides high-level planning and operational best practices for defining local backup and recovery services.

## Phase 4: Deploy

The Deploy phase again implements the plans derived from the effort of the previous three phases. If your organization has selected to augment its current backup and recovery operations with Data Protection Manager 2006, you can find deployment guidance on Microsoft TechNet in the [Data Protection Manager 2006 Planning and Deployment Guide](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/25b59474-1124-4ca1-9a0f-921b28bc0025.mspx).

## Further Information

For more information on backup and restore, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “branch office data backup and recovery.”

To see how Microsoft addresses data protection, go to <http://www.microsoft.com/technet/itshowcase/content/dpmtcs.mspx>.

## Checkpoint: Centrally Managed Data Backup for Branch Offices

|  |  |
| --- | --- |
| X | Requirement |
|  | Created a centralized data backup plan and a recovery plan for branch offices in your organization. |
|  | Implemented a backup and recovery plan for centralized control of backup and recovery operations, either via network-centralized tools or operational guidelines for local backup and recovery, with defined service levels. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Centrally Managed Data Backup for Branch Offices capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for managing data at branch offices.

Go to the [next Self-Assessment question](#_Requirement:_Data_Protection_1).

# Requirement: Backup, Restore, and Defined Recovery Times for Servers

## Audience

You should read this section if you do not have a service level agreement (SLA) for system backup and restore and defined recovery times for 80 percent of your servers.

## Overview

In the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized*, you read about data backup and restore services for critical servers. To move from the Standardized level to the Rationalized level, you need to extend your backup and restore capabilities to 80 percent or more of your servers. You also need to define and track recovery times through SLAs.

This section of the *Core Infrastructure Optimization Resource Guide for Implementers: Standardized to Rationalized* summarizes the topics covered in the Basic to Standardized guide because the standards that apply to your critical servers apply equally to non-critical servers, and recovery times at the Rationalized level are defined.

The following guidance is based on the [Windows Server System Reference Architecture implementation guides for Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx) and [Microsoft Operations Framework (MOF) Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx) guides.

## Phase 1: Assess

The Assess phase examines the business need for extending your backup and recovery operations to all servers and takes inventory of the current backup and recovery processes in place for critical servers. Backup activities ensure that data is stored properly and available for both restore and recovery, according to business requirements. The design of backup and recovery solutions needs to take into account business requirements of the organization as well as its operational environment.

## Phase 2: Identify

The goals of the Identify phase of your backup and recovery solution are to identify the targeted data repositories, take baseline measures of the current recovery times, establish defined recovery times and corresponding service level agreements (SLAs), and derive high-level business requirements to achieve defined recovery times. Defining recovery times and SLAs for backup and recovery services share the same process and guidance with defining SLAs for the requirement of [service monitoring](#_Service_Level_Agreement) in this guide. Any backup and recovery solutions that are deployed must be predictable, reliable, and capable of complying with regulations and processing data as quickly as possible.

Challenges that you must address in managing data include:

* Managing growth in the volumes of data.
* Managing storage infrastructure to improve the quality of service (QoS) as defined by SLAs, while reducing complexity and controlling costs.
* Integrating applications with storage and data management requirements.
* Operating within short, or nonexistent, data backup windows.
* Supporting existing IT systems that cannot run the latest technologies.
* Managing islands of technology that have decentralized administration.
* Assessing data value so that the most appropriate strategies can be applied to each type of data.

[Microsoft Operations Framework (MOF) Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx) provides additional details for the Identify phase of Backup and Recovery operations.

For detailed information about best practice service level management, read the [MOF Service Level Management guidance](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx).

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase for the Rationalized level follows the same steps outlined in the *Core Infrastructure Optimization Resource Guide for Implementers: Basic to Standardized* guide. As you extend services to all servers at the Rationalized level, you should take into account several data points to determine the appropriate backup and recovery solution for your organization. These requirements can include:

* How much data to store.
* Projected data growth.
* Backup and restore performance.
* Database backup and restore needs.
* E-mail backup requirements.
* Tables for backups and restores.
* Data archiving (off-site storage) requirements.
* Identification of constraints.
* Select and acquire storage infrastructure components.
* Storage monitoring and management plan.
* Testing the backup strategy.

See [Microsoft Operations Framework Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx) for more details.

### Backup Plan

In developing a backup and recovery plan for critical servers you need to consider these factors:

* Backup mode
* Backup type
* Backup topology
* Service plan

Microsoft’s Data Protection Manager (DPM) is a server software application that enables disk-based data protection and recovery for file servers in your network. The [DPM Planning and Deployment Guide](http://www.microsoft.com/downloads/details.aspx?FamilyId=034FCFD6-DEFE-44BC-BF18-F4A22CB17D95&displaylang=en) contains a wealth of information on setting up a backup and recovery plan.

### Recovery Plan

Even the best backup plan can be ineffective if you don’t have a recovery plan in place. Following are some of the elements of a good data recovery plan.

* Verify backups.
* Back up existing log files before performing any restoration.
* Perform a periodic fire drill.
* Create a disaster kit.

### Recovery Times

Your SLAs should have defined recovery times for your servers. These times need to be renegotiated periodically as equipment and services expand. You can also use your records of data recovery incidents and the improvement over time of your ability to restore servers to operation to negotiate recovery times.

## Phase 4: Deploy

After the appropriate storage infrastructure components are in place and the backup and recovery service plan is defined, your organization can install the storage solution and associated monitoring and management tools into the IT environment.

## Further Information

For more information on backup and recovery solutions, visit the [Data Protection Manager 2006](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/default.mspx?mfr=true) and [Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx) Web sites.

To see how Microsoft addresses server backup and restore, go to <https://www.microsoft.com/technet/itshowcase/content/dpmtcs.mspx>.

## Checkpoint: Backup, Restore, and Defined Recovery Times for Servers

|  |  |
| --- | --- |
| X | Requirement |
|  | Created a data backup plan and a recovery plan for 80 percent or more of all servers in your organization. |
|  | Used drills to test your plans and validate defined recovery times. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Backup, Restore, and Defined Recovery Times for Servers capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for backup, restore, and recovery for servers.

Go to the [next Self-Assessment question](#_Requirement:_Security_and_8).

Capability: Security Process

# Introduction

Security process is a key element of infrastructure optimization, and security must be part of the design criteria for all procedures and technologies highlighted by the Infrastructure Optimization Model. The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in Security Process.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  No consistent risk assessment processes  An incident response plan is in place, but not fully documented  Only standard identity protection technology is used  **IT Challenges**  Limited PC security  The process for updating security on all network connected IT assets is undocumented | **Projects**  Continue optimizing defense-in-depth security policies  Develop and implement two-factor identity and access management policies  Develop a process to manage security requirement testing on all acquired or developed software  Establish a standard and repeatable procedure for classifying sensitive data | **Business Benefits**  Problems and incidents are reduced and remaining occurrences are resolved faster  Improved information security and identity protection helps protect business from threats, regardless of device  **IT Benefits**  Automated services and tools free up resources to implement new services or optimize existing services  Proactive IT operations resolve problems earlier to avoid reducing user productivity |

The Rationalized level of optimization requires that your organization has defined procedures for risk management, incident management and response, and application testing.

# Requirement: Two-Factor User Authentication, Standard Security Review for New Software Acquisitions, and Data Classification Processes

## Audience

You should read this section if you do not have plans in place for security policies, risk assessment, incident response, and data security.

## Overview

Most organizations know that it is important to protect their data and resources from loss or damage due to theft, human or computer error, malicious intent, or any number of other events. You can take steps to limit the opportunities for loss or damage to occur. You can also establish policies and procedures to respond to and minimize the effects of the loss or damage to your IT environment. The Rationalized level in this guide deviates somewhat from the [Core Infrastructure Optimization Online Self-Assessment](http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx) and focuses on the following topics: two-factor user authentication, standard security review for new assets, and data classification processes.

## Phase 1: Assess

The Assess phase should determine the appropriate security needs for your organization and which processes are currently in place. Security requirements can vary dramatically from company to company or institution to institution based, for example, on size, industry or field, or regional laws and regulations. Gathering the requirements of your organization will allow you to define an appropriate security process.

## Phase 2: Identify

During the Identify phase, an organization will examine the tools and procedures currently in place and determine what the security requirements are for its organization. During this phase, you will gather security policies that are currently implied or enforced, in addition to technology components already in use or at your disposal. You will also gather any external requirements based on laws or regulations for your region or industry.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase moving to the Rationalized level of optimization highlights specific areas of improvement.

### Two-Factor Authentication

Single secrets such as passwords can be effective security controls. A long password of more than 10 characters that consists of random letters, numbers, and special characters can be very difficult to crack. Unfortunately, users cannot always remember these sorts of passwords, partly due to fundamental human limitations.

Two-factor authentication systems overcome the issues of single secret authentication by the requirement of a second secret. Two-factor authentication uses a combination of the following items:

* Something that the user has, such as a hardware token or a smart card.
* Something the user knows, such as a personal identification number (PIN).

Smart cards and their associated PINs are an increasingly popular, reliable, and cost-effective form of two-factor authentication. With the right controls in place, the user must have the smart card and know the PIN to gain access to network resources. The two-factor requirement significantly reduces the likelihood of unauthorized access to an organization’s network.

Smart cards provide particularly effective security control in two scenarios: to secure administrator accounts and to secure remote access. This guide concentrates on these two scenarios as the priority areas in which to implement smart cards.

Because administrator-level accounts have a wide range of user rights, compromise of one of these accounts can give an intruder access to all network resources. It is essential to safeguard administrator-level access because the theft of domain administrator-level account credentials jeopardizes the integrity of the domain, and possibly the entire forest, together with any other trusting forests. Two-factor authentication is essential for administrator authentication.

Organizations can provide an important additional layer of security if they implement smart cards for users who require remote connectivity to network resources. Two-factor authentication is particularly important with remote users because it is not possible to provide any form of physical access control for remote connections. Two-factor authentication with smart cards can increase security on the authentication process for remote users who connect through virtual private network (VPN) links.

For detailed information on two-factor authentication, go to <http://www.microsoft.com/technet/security/guidance/networksecurity/securesmartcards/default.mspx>.

### Standard Security Review for New Software Acquisitions

At the Rationalized level, all software acquisitions in your organization should follow a program to enable standard security review. Best practice processes for performing security reviews of IT systems are outlined in the [ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=) standard. ISO/IEC 17799:2005 establishes guidelines and general principles for information systems acquisition, development, and maintenance, including:

* Security requirements of information systems.
* Correct processing in application systems.
* Cryptographic controls.
* Security of system files.
* Security in development and support processes.
* Technical vulnerability management.

For more information about the standard and to obtain the documentation, visit the [ISO/IEC 17799:2005 Information technology -- Security techniques -- Code of practice for information security management](http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=39612&ICS1=35&ICS2=40&ICS3=) Web site.

### Data Classification Processes

Data classification and protection deals with how to apply security classification levels to the data either on a system or in transmission. This solution category also deals with data protection in terms of providing confidentiality and integrity to data that is either at rest or in transmission. Cryptographic solutions are the most common method that organizations use to provide data protection.

#### Compliance Impact

Data classification is important to compliance because it informs users about what levels indicate the relative importance of the data, how they must handle the data, and how they must safeguard and dispose of it. High, medium, and low are typical data classification examples that indicate the relative impact of the data on business. The military classification system of Top Secret, Secret, Confidential, and Un-Classified may also apply in some organizations.

All compliance guidelines require file protection and encryption of sensitive information, whether at rest or in transit. The compliance process creates enormous amounts of sensitive data, primarily in nonstructured applications such as Microsoft Office Word and Office Excel files. Control and protection of this compliance data is very important because it contains complete details of an organization's known weaknesses and vulnerabilities.

#### Microsoft Resources

Microsoft provides several resources for data classification and data protection. For example, the combined use of Information Rights Management (IRM), which extends the Windows Rights Management Services in Microsoft Office 2003 applications and in Microsoft Internet Explorer, as well as Windows Rights Management Services (RMS) technologies help you to both classify and protect the data in your organization. RMS applies encryption-based, policy-driven protection that travels with the information wherever it goes.

Additional data protection technology solution examples include Internet Protocol security (IPsec) and Encrypting File System (EFS). IPsec provides data integrity and encryption to IP traffic, whereas EFS encrypts files stored in the file systems of Microsoft Windows 2000 Server, Windows XP Professional, and Windows Server 2003. Microsoft provides the following guidance on these data classification and protection solutions:

* For more information about planning for regulatory compliance, see the *Regulatory Compliance Planning Guide* at <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/compliance/rcguide/4-11-00.mspx>.
* For more information about Windows Rights Management Services partner offerings, see [Windows Rights Management Services Partners](/windowsserver2003/partners/rmspartners.mspx) at [www.microsoft.com/windowsserver2003/partners/rmspartners.mspx](http://www.microsoft.com/windowsserver2003/partners/rmspartners.mspx).
* For more information about RMS, see [Windows Rights Management Services](/rms) at [www.microsoft.com/rms](http://www.microsoft.com/rms).
* For more information about the information rights management capabilities of Office 2003, see [Information Rights Management in Microsoft Office 2003](/technet/prodtechnol/office/office2003/operate/of03irm.mspx) at [www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx](http://www.microsoft.com/technet/prodtechnol/office/office2003/operate/of03irm.mspx).
* For information about IPsec, see the [IPsec](/windowsserver2003/technologies/networking/ipsec/default.mspx) Web site at [www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx](http://www.microsoft.com/windowsserver2003/technologies/networking/ipsec/default.mspx).
* For information about how to use IPsec and Group Policy to isolate servers and domains, see [Server and Domain Isolation Using IPsec and Group Policy](http://go.microsoft.com/fwlink/?linkid=33945) at <http://go.microsoft.com/fwlink/?linkid=33945>.
* For information about how to use EFS to protect data, see [Protecting Data by Using EFS to Encrypt Hard Drives](/technet/security/smallbusiness/topics/cryptographyetc/protect_data_efs.mspx) at [www.microsoft.com/technet/security/smallbusiness/topics/cryptographyetc/protect\_data\_efs.mspx](http://www.microsoft.com/technet/security/smallbusiness/topics/cryptographyetc/protect_data_efs.mspx).
* For more information about EFS, see [The Encrypting File System](http://go.microsoft.com/fwlink/?linkid=46681) at <http://go.microsoft.com/fwlink/?linkid=46681>.
* For information about how to protect sensitive information from theft, see [Protecting Sensitive Information from Theft on Windows XP Professional in a Workgroup](/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx) at [www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx](http://www.microsoft.com/technet/security/smallbusiness/prodtech/windowsxp/efsxppro.mspx).

## Phase 4: Deploy

Evaluated and approved security process improvements are implemented in the Deploy phase. It is important to perform usability tests as they pertain to tightening of security policy and periodic fire drills to ensure data processes are efficient.

## Further Information

For more information on developing security operations and process standards, go to the Security Guidance Portal on Microsoft TechNet at <http://www.microsoft.com/technet/security/guidance>.

## Checkpoint: Two-Factor User Authentication, Standard Security Review for New Software Acquisitions, and Data Classification Processes

|  |  |
| --- | --- |
| X | Requirement |
|  | Developed and implemented two-factor identity and access management policies. |
|  | Developed a process to manage security requirement testing on all acquired or developed software. |
|  | Established a standard and repeatable procedure for classifying sensitive data. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Two-Factor User Authentication, Standard Security Review for New Software Acquisitions, and Data Classification Processes.

We recommend that you follow additional best practices for security processes addressed at the [Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx).

Go to the [next Self-Assessment question](#_Requirement:_Security_and_9).

Capability: ITIL/COBIT-based Management Process

# Introduction

Best practice processes must be defined for all tasks highlighted in the Infrastructure Optimization Model in order to receive maximum benefit and performance. The following table lists the high-level challenges, applicable solutions, and benefits of moving to the Rationalized level in ITIL/COBIT-based Management Process.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  SLAs are informal or implied  Informal configuration management consists of basic build checklists and spreadsheets  **IT Challenges**  Informal release management | **Projects**  Implement service level management across IT operations  Implement best practice release management  Optimize network and system administration processes  Implement best practice job scheduling | **Business Benefits**  Proactive IT operations resolve problems earlier to avoid reducing user productivity  **IT Benefits**  Automated services and tools free up resources to implement new services or optimize existing services  Formal SLAs connect IT to the business by improving IT’s credibility |

The Rationalized level of optimization requires that your organization has defined procedures for incident management, problem management, user support, configuration management, and change management.

# Requirement: Operating, Optimizing, and Change Processes

## Audience

You should read this section if you do not have processes for service level management, release management, systems administration, network administration, and job scheduling.

## Overview

Infrastructure optimization goes beyond products and technologies. People and processes compose a large portion of an organization’s IT service maturity. A number of standards and best practice organizations address the areas of people and process in IT service management. [Microsoft Operations Framework (MOF)](http://www.microsoft.com/mof) applies much of the knowledge contained in the [IT Infrastructure Library (ITIL)](http://www.itil.co.uk/) and [Control Objectives for Information and related Technology (COBIT)](http://www.isaca.org/) standards and makes them actionable and achievable for Microsoft customers.

## Phase 1: Assess

The goal of the Assess phase in operations management is to evaluate the organization’s current capabilities and challenges. To support the operations assessment process, Microsoft has developed the Microsoft Operations Framework (MOF) Service Management Assessment (SMA) as part of the [MOF Continuous Improvement Roadmap](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/index.mspx), and a lighter online version called the [MOF Self-Assessment Tool](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/moftool.mspx).

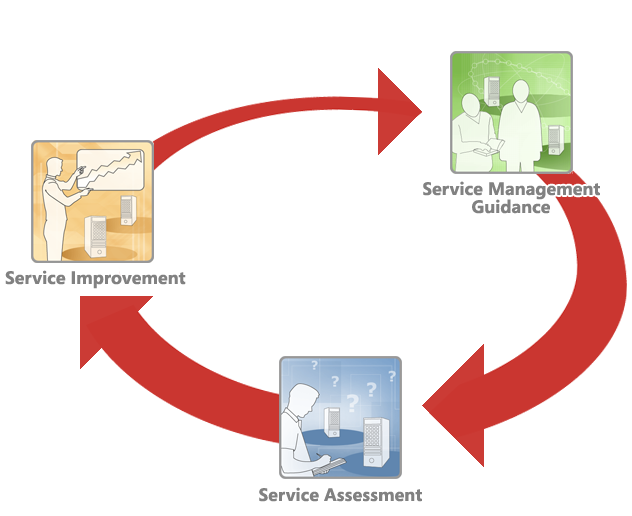


Figure 16. MOF life cycle of continuous improvement

The MOF Service Management Assessment is focused on enhancing the performance of people and IT service management processes, as well as enabling technologies that improve business value. All recommendations generated as a result of the SMA are detailed and justified in business value, and a detailed service improvement roadmap is provided, supported by specific key performance indicators to monitor progress as improvements are implemented.

## Phase 2: Identify

The results of the MOF Service Management Assessment form the basis of the Identify phase. The Assessment will often expose several areas of potential improvement in IT operations. During the Identify phase, we consider these results and prioritize improvement projects based on the business need. Tools and job aids are included in the MOF Continuous Improvement Roadmap to assist with this prioritization.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase for operational improvement relies on the identified and prioritized areas for improvement. The MOF Service Improvement Program (SIP) guidance enables this phase. SIP is split into two major areas of focus: specific MOF/ITIL process improvement and service improvement guidance. This guidance is delivered through a tool that assists users in identifying their specific trouble points, provides focused guidance for remediation, and is supported by key performance indicators to measure process improvement.

### Recommended Processes for Moving to the Rationalized Level

The recommendations in this section are based on common issues found at the Standardized level and areas of improvement sought by the Rationalized level. These are only recommendations and may be different for your specific organization or industry.

Although the Standardized level brings an increased use of tools for managing and monitoring IT operations and infrastructure, plus an environment in which such processes as change management, configuration management, and release management are standardized and predictable, there is room for improvement in key areas. Service level management is rudimentary with service level agreements (SLAs) that are informal or only implied. Configuration management is informal and typically consists of basic build checklists and spreadsheets, and release management is not well defined and lacks rigor.

The Rationalized infrastructure is where the costs involved in managing desktops and servers are at their lowest and processes and policies have been optimized to begin playing a large role in supporting and expanding the business. Security is very proactive, and responses to threats and challenges are rapid and controlled. The use of zero touch deployment helps minimize cost, the time to deploy, and technical challenges. The number of images is minimal, and the process for managing desktops is very low touch. These customers have a clear inventory of hardware and software and only purchase the licenses and computers they need. Security is extremely proactive with strict policies and control, from the desktop to server to firewall to extranet.

Microsoft provides [Microsoft Operations Framework (MOF)](http://www.microsoft.com/mof) as an iterative model for defining and improving IT operations. MOF defines service management functions (SMFs) as logical operational functions within an IT organization. The SMFs are grouped together into four broad areas, or quadrants: Changing, Operating, Supporting, and Optimizing. This guide highlights areas to improve that are typically found in organizations at the Standardized level of optimization:

* Service Level Management
* Release Management
* System Administration
* Network Administration
* Job Scheduling

Depending on the organization, improvements to these service management functions might or might not have the greatest impact on operational effectiveness and improvement. We recommend that your organization at a minimum completes the [online self-assessment](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/moftool.mspx), and preferably a full [Service Management Assessment](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/index.mspx), to identify the most important areas requiring process or service improvements.

### Service Level Management

[Service Level Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx#ENIAC) (SLM) is a critical process that aligns business needs with the delivery of IT services. It provides the interface with the business that allows the other SMFs to deliver IT solutions that are in line with the requirements of the business and at an acceptable cost. Its primary goal is to successfully deliver, maintain, and improve IT services.

SLM is used to align and manage IT services through a process of definition, agreement, operation measurement, and review. The scope of SLM includes defining the IT services for the organization and establishing SLAs for them. Fulfilling SLAs is ensured by using underpinning contracts (UCs) and operating level agreements (OLAs) for internal or external delivery of the services. Introducing Service Level Management into a business will not give an immediate improvement in the levels of service delivered. It is a long-term commitment. Initially, the service is likely to change very little; but over time, it will improve as targets are met and then exceeded.

If an organization wants to implement Service Level Management, it must first assess what services IT provides to the organization’s customers and determine what existing service contracts are currently in place for these services. This assessment can make the IT service department aware, often for the first time, of the full range of services it is expected to deliver. With the information gained through this exercise, the organization can then develop and implement the full benefits of the Service Level Management process.

Service Level Management requires that the IT organization fully understand the services it offers. Implementing Service Level Management follows these steps:

* Creating a service catalog.
* Developing SLAs.
* Monitoring and reporting.
* Performing regular service level reviews.

SLAs are developed in line with the requirements and priorities of the services documented in the service catalog, the requirements specified under negotiation of the SLAs, the monitoring of the service against the agreement criteria, and the reporting and reviewing of this information to highlight and remove failures in the levels of performance of the service.

## Phase 4: Deploy (Service Level Management)

### Setup Activities

Setup activities are a series of appraisal steps carried out at the beginning of a Service Level Management project. These preliminary steps help the business determine if there is a need for Service Level Management and if it has the resources to implement it. As part of this process, the IT department establishes a baseline for the business by taking a snapshot of the existing services and management activities. The final step is to analyze the information collected in the previous steps and use the results to plan the implementation of Service Level Management for maximum benefit to the business.

### Creating a Service Catalog

The service catalog lists all of the services currently being provided, summarizes service characteristics, describes the users of the service, and details those responsible for ongoing maintenance.

A service is defined by the business organization's perception. For example, e-mail may be a service and printing may be a service, regardless of the number of service components required to deliver the service to the end user.

Formalizing a service catalog is an important step in that it creates an officially recognized record. Making the service catalog an official record within the organization places it under change control. This is important since the record is valuable only if it is maintained and accurate.

There are many ways to formalize a service catalog. When determining which method is most suitable for use, consider how you want to view, report against, and use the service catalog. A service catalog can be stored as part of the configuration management database (CMDB) either as one component (the service catalog) or as its services. Microsoft applications, such as Microsoft Excel or Microsoft Access, can be used to record the services and such details as the components, effects, priorities, and SLAs and SLOs. If the tool selected allows the service catalog to be part of the CMDB, then this can add value by integrating the information in the service catalog with the configuration item (CI) in the CMDB. This can then be used to add value to the Change Management SMF, Incident Management SMF, and all other SMFs using the CMDB.

### Developing Service Level Agreements (SLAs)

An SLA is an agreement between the IT service provider and the customer/user community. The SLA formalizes customer/user requirements for service levels and defines responsibilities of all participating parties.

The steps for creating an SLA are:

* **Define the type of SLA.** For example, is it an internal, external, operating level, or multi-service level agreement?
* **Define the SLAs.** For example, what levels of service will be delivered, including such measurable things as availability, responsiveness and performance, integrity and accuracy, and security.
* **Negotiate and agree on SLAs.** For example, determine whether what has been agreed to can be delivered at a reasonable cost to the business and to the IT department.
* **Document the SLA.** For example, record in writing what has been agreed to and who is involved.

### Aligning SLA, OLA, and UC Commitments

Underpinning contracts (UCs)—legally binding contracts with a third-party service provider on which service deliverables for the SLA have been built—and operational level agreements (OLAs)—an internal agreement supporting the SLA requirements—must have service metrics that are aligned with the SLA commitment.

### Service Level Monitoring

Service level management requires an ongoing cycle of agreeing, monitoring, and reporting on IT service achievements and taking appropriate actions to balance service levels with business needs and costs.

When the SLAs are agreed on and in place, the next stage in effective Service Level Management is to monitor the performance of the services against criteria specified in the service level objectives (SLOs). There are various methods of monitoring Service Level Management, but the main concern is if the performance of any of the criteria breaches or comes near to breaching the SLA.

### Service Level Agreement Review

The SLA Review is one of the four MOF operations management reviews (OMRs). It is a key management checkpoint and occurs at specified intervals (as documented in the SLA). This review is meant to ensure that the business and IT have an opportunity to assess performance against SLA objectives and to review the operation of the SLA. The SLA Review is designed to involve high-level management in the review process, ensuring that involvement and communication is present from both IT and the business in all future decisions regarding the delivery of the service.

### Release Management

The [Release Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfrelmg.mspx) service management function (SMF) is responsible for deploying changes into an information technology (IT) environment. After one or more changes are developed, tested, and packaged into releases for deployment, release management is responsible for introducing these changes and managing their release. Release management also contributes to the efficient introduction of changes by combining them into one release and deploying them together.

The goal of the release management process is to ensure that all changes are deployed successfully into the production IT environment in the least disruptive manner. Therefore, release management is responsible for:

* Driving the release strategy, which is the overarching design, plan, and approach for deployment of a change into production in collaboration with the change advisory board (CAB).
* Determining the readiness of each release based on release criteria (quality of release, release package and production environment readiness, training and support plans, rollout and backout plans, and risk management plan).

Release management:

* Provides a packaged release for all changes deployed into production and only deploys changes approved by change management.
* Needs change management to approve changes and track them throughout the release process.
* Ensures that, as changes are made, those changes are reported to configuration management for entry in the CMDB.
* Needs configuration management information to build and verify valid test environments in the development phase of the new release.
* Needs configuration management to assess the impact of changes to the IT environment and to provide a definitive store for the release package.

## Phase 4: Deploy (Release Management)

### Release Planning

The first step in the release process is the creation of a plan identifying the activities and the resources required to successfully deploy a release into the production environment. That plan involves determining what tasks need to be done, when they need to be complete (timescale), and what their priority is in relation to other tasks. Once these issues are fully understood, the release manager can draw up a detailed plan of activities and assign appropriate resources to the project. In Release Management, the release manager role is responsible for building a release (project) plan for each RFC approved by change management.

### Release Building

Once the release plan is agreed on, members of the release team identify and develop the processes, tools, and technologies required to deploy the release into production. Although most (if not all) releases could be deployed into production manually, a number of tools and technologies can be used to perform the same task. To make best use of time and resources, the release team should identify the tools and technologies that will enable it to automate as much of the deployment process as possible.

Once the release mechanism has been selected, the release team creates a release package that contains the processes, tools, and technologies required to deploy the release into production by using the selected mechanism and to remove it from production should that become necessary.

For some releases, the release package may simply consist of a set of documented installation and removal procedures.

The completed release package should be tested in a lab environment to give the release team a degree of confidence that it will work correctly when used in production. Assuming that testing completes successfully, the release and the contents of the release package are then placed under the control of change management.

### Acceptance Testing

Up to this point, the emphasis of testing has been to confirm that the release and release package work correctly within a development environment. Acceptance testing allows developers and business representatives to see how the release and release package perform together in an environment that closely mirrors production. In some cases, pilot testing is required to build the confidence necessary to proceed to a organization-wide deployment of the change.

Although testing in a simulated production environment provides the release team with a degree of confidence in the release, it does not guarantee that the release will perform well in production, where conditions may be significantly different. In this respect, it may be necessary to perform a number of controlled tests in the production environment to confirm that the release meets expectations. Piloting a release in a production environment carries a number of risks to that environment and should only be performed if the recovery procedures contained in the release package have been proven in the test environment.

### Release Preparation

After pilot and acceptance testing has been completed, the next step is to prepare the production environment for the release, move through the preparation process, and agree on the action to be taken—either to move to the Release Readiness Review or to return the release to the change owner or release manager for additional work.

The release manager, change manager, and change owner are the primary participants in the Release Readiness Review discussion, but it also may include representatives of other interested groups, such as the test teams, service desk, and user community (depending on the nature and size of the release).

Although a release may have failed a number of tests, both in the lab and in the production environment, the failures may not be significant enough to prevent deployment. Even if there are implications for the production environment, there may be a number of compelling business reasons why the release must be deployed.

For example, in a business-to-business commerce site, one feature—such as automated sign-up—may not work. It is easy to remove this feature and use a manual workaround. Therefore, the team might choose to proceed without this feature.

The testing experiences and lessons learned (in addition to any workarounds developed) are captured and documented. If issues were picked up during testing that affect the user community or service levels, it is necessary to discuss workarounds and expected problems with the service desk representatives and to ensure that the workarounds will be available to the service desk prior to deployment. Additional RFCs might need to be initiated in order to make the release work as planned. In either case, the change log needs to be updated with the decision and any other supporting information.

### Release Deployment

The process of deploying the release into the production environment depends on the type and nature of the release and on the selected release mechanism. In all cases, however, the release manager should be provided with status reports and, where appropriate, tools and technologies that will enable tracking and monitoring of deployment progress. As changes are made to IT components during deployment, corresponding changes must be made to the configuration items and relationships modeling them in the CMDB.

Once the release is deployed, the release manager confirms that it is working correctly before proceeding with further deployments. For some releases, technical support staff can obtain confirmation by using a number of tools and technologies; for others, the release manager may need to ask the service desk to contact individual users for their feedback and comments.

If the release fails to meet expectations or if serious problems are encountered during deployment, problem management may be needed to help identify and diagnose the root cause of the problem. If a suitable fix or workaround can be found, this should be documented and a request for change created to deploy it into the production environment. If not, it may be appropriate to use the backout procedures to remove the release from that environment.

Once the release deployment phase is complete, the release process should ensure that any results and information about any workarounds or RFCs raised in support of the release are recorded. If the release needs to be backed out, this should also be recorded, including any information that supports this decision.

### System Administration

The [System Administration](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsysad.mspx) function performs Security Administration, Service Monitoring and Control, Job Scheduling, Network Administration, Directory Services Administration, Print and Output Administration, and Storage Management. The way in which one designs, develops, and implements this function will be determined by the size and architecture of the organization. Large organizations will have clearly defined models while smaller organizations will be likely to consolidate functions in order to maintain the health and operational capabilities of the systems.

The objective of the System Administration SMF is to administer a computing environment on a day-to-day basis. This entails managing and providing operational support for various elements within the production environment.

The System Administration function is responsible for providing administrative services in support of computing environments that contain both centralized and distributed hardware.

The System Administration function may also provide assistance with the functional administration of other SMFs that they are not directly responsible for implementing and managing. This assistance may include:

* First-level performance and capacity monitoring for the Service Monitoring and Control function.
* The day-to-day functional administration of account management, including adding, deleting, or moving accounts. Enquiries for resources such as printers and security access privileges for Directory Services Administration and Security Administration.
* Management of resources used to produce printed reports and output for Print and Output Management.
* The administrative tasks required to back up and restore critical data.
* Enforcing a security policy for protecting data and shared network resources including files, folders, and printers.

## Phase 4: Deploy (System Administration)

### Implementing the Centralized Administration Model

In the centralized administration model, all or most of the operations and support functions are centrally located in a single site, or sites. With the maturation of local area, wide area, distributed, and client server computing and their supporting networks, more and more organizations have made great strides toward centralizing support for installed resources, applications, and solutions.

Bandwidth to remote sites and branch offices is more widely available and affordable. Basic technologies that support branch office computing (transmission protocols, remote access tools, headless servers, and so on) have improved to the point where each branch office no longer needs its own separate support staff. Companies are thus increasingly able to centralize the fundamental support functions required to maintain the availability, reliability, day-to-day support, and management of systems that are distributed to the remote sites or branch offices.

Centralized administration typically assumes that all or most of the computing systems and resources being managed (administered) are centrally located. Although this is increasingly true, there continues to be cases where specific solutions (that is, custom applications, specialized databases, and so on) are not centralized in the corporate data center, but instead are distributed to the remote branch or site. This distribution of some applications and databases does not prevent taking a centralized approach to the administrative model.

### Implementing the Centralized/Remote Administration Model

The centralized/remote administration model achieves most of the benefits of the completely centralized model. Most administration continues to be performed at the central location (for example, central data center), thereby retaining the greatest control and consolidation of resources necessary to execute the administrative function.

Some control and resource consolidation is given up, however, due to the requirement of maintaining a remote data center environment with at least a minimal localized administrative presence. Remedial system maintenance requirements on the distributed system may include system updates that require a reboot of the computer, as well as tape-backup and storage duties. There may be additional local-site administrative requirements, depending on the application or specific system being managed; you'll have to decide what specific responsibilities are necessary based upon your technology application.

The centralized/remote administration model describes systems that are distributed to remote locations with all major administrative control remaining at the central location. As stated above, there now needs to be a data center presence in the remote or regional location to house the servers or storage units. This implies that you now incur the cost of the data center infrastructure, which includes the physical plant, floor space, power, wiring, HV/AC, and security components.

If the technology application evolves to the point where this model no longer remains viable (that is., no longer meets the service level agreements) or is no longer cost-effective, you may need to move to a distributed administrative model. In a distributed administrative model, the computing resources as well as the people resources are physically located at the remote location. This model is described in the next section.

### Implementing the Centralized/Delegated Administration Model

This model attempts to embrace the best of the centralized and remote administration models with all of their inherent features and benefits, yet also realizes some of the benefits of the distributed administration model. These benefits are achieved by pushing a relatively small and specialized subset of administrative tasks and responsibilities to the local branch offices and remote sites.

As with the centralized model, the primary administrative function and administrative workforce reside at the corporate (central) data center—all administrative direction and control originate from this location. The centralized resources continue to manage the centralized, data center-based network servers and services; these centralized resources also continue to remotely administer services across the network where possible, reasonable, and applicable.

Certain circumstances dictate the need to distribute specific services, servers, and resources; in these cases it may also be prudent and/or more efficient to allow some of the administrative tasks to be performed at the regional or remote locations. This is done by delegating very specific authority to the remote location resources. "Very specific authority" refers to a small subset of administrative rights and access that allow the remote administrators to perform specific, discrete tasks.

### Implementing the Distributed Administration Model

Unlike the other models, distributed administration relies on full-support resources located in remote sites or branch offices. Resources at remotely located sites perform the fundamental (although critical) support functions necessary to maintain the health, availability, and reliability of systems distributed to those sites.

There may continue to be business drivers for maintaining systems that are distributed to remote locations. Some of these drivers may be related to performance, scalability, a specific type of application, or the cost or availability of network bandwidth that would support a centralized solution.

Computing and people resources are completely distributed to the remote offices and regional sites. As a result, the organization may realize much better local site performance for specific technology applications.

### Implementing the Distributed Administration of Centralized Data Centers Model

The fifth system administration possibility, referred to here as the "follow-the-sun" model, could also be called the "distributed administration-centralized data center" (more than one) model.

"Following the sun" in this context means providing support globally 7 days a week, 24 hours a day by transferring the responsibility for this support to different regions around the world as some offices close for the day and others open.

This model is somewhat unique and is not as widely implemented as the four basic models previously described. It should be noted, however, that companies have tried, or are currently trying, to get this model to work in their organizations.

### Network Administration

The [Network Administration](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfnetadm.mspx) service management function focuses on operating networks, which are the infrastructure components through which computer systems and shared peripherals communicate with each other. It is the most basic level of an IT infrastructure; without network facilities, there is no infrastructure, just a collection of individual computers.

The goal of the Network Administration SMF is to provide and reference a solid foundation of processes for administering a network environment on a day-to-day basis. This entails managing and providing operational support for various elements within the production environment. The SMF’s objectives include providing planning and deployment services to expand existing network facilities, as well as support services to troubleshoot and repair faults in the network environment. Through effective implementation of the Network Administration SMF, IT organizations can expect to:

* Improve their deployment of network infrastructure.
* Improve troubleshooting processes and associated incident-management processes.
* Increase network reliability.
* Enhance availability of IT solutions and services.

A typical network consists of hardware—including cabling, routers, switches, hubs, physical servers, and other components—and the software or firmware that controls the manner in which the hard components are utilized. In the networking model described by Open Systems Interconnection (OSI), the typical IT infrastructure is constructed in layers, from basal components that are used by all services at the bottom of the stack, to specialized applications at the top.

The layers making up the OSI stack are (from the top, down):

1. Application
2. Presentation
3. Session
4. Transport
5. Network
6. Link (Data Link)
7. Physical

Network administration is typically involved with the first three layers of the stack, which mostly consist of hardware. There is some overlap between network and system administration at the transport level, which includes the linking and networking protocols that enable the transfer of data from one point to another. From the MOF perspective, management of such services as DNS, WINS, and DHCP provides the basic name resolution services required by fully featured IT services. Depending upon the organization, these core services may also be included as network service functions. Since DNS, WINS, and DHCP run on servers, network servers are sometimes included among the hardware components managed by the Network Administration SMF.

## Phase 4: Deploy (Network Administration)

### Maintaining a Network

Operating the network infrastructure is largely a matter of monitoring its performance, evaluating that against expected norms, and generating work items to troubleshoot if performance drops off. Most hardware components within a network should operate without hands-on maintenance or intervention within the manufacturer’s specifications for mean time between failure and other performance criteria. The MOF Capacity Management SMF provides details for capacity planning that will help the network design team in optimizing network performance.

The server-based components of the network do require periodic attention, however. These components require regular backups, where applicable, and evaluations of storage or capacity requirements, in accordance with the Storage Management SMF.

### Supporting a Network

Network support is closely aligned with activities in the Supporting Quadrant, particularly the Incident Management SMF and Problem Management SMF. Through the incident resolution process described in the Incident Management SMF, IT networking specialists correct network errors, develop workarounds, and prevent or mitigate impending network issues. Although the generic process for resolving incidents is described in the Incident Management SMF guidance document, network-specific processes for troubleshooting are provided in the following sections.

### Job Scheduling

The [Job Scheduling](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfjobsc.mspx) Service Management Function (SMF) is concerned with ensuring the efficient processing of data at a pre-determined time and in a prescribed sequence to maximize the use of system resources and minimize the impact to online users. A batch process is a system interaction with a database that runs in the background and in a sequential manner without interaction from an end user. The execution of batch processes may be automated or manually initiated. Batches are usually executed after business hours when user interaction with the system is low.

Batch runs typically require their own architecture as they tend to be resource-intensive and long running, repetitive processes. The process usually involves reading large amounts of data from a database, processing the data, and returning the results back to a database. This process is accomplished through the execution of scripts.

Types of batch jobs that organizations execute include:

* Financial management reports
* Marketing reports
* Supply chain management reports
* Inventory reports
* Invoice reports
* Customer account processing (monthly account billing, and so on)
* Automated backups of system and application data
* System processing summaries and capacity planning reports

## Phase 4: Deploy (Job Scheduling)

### Batch Architecture

A batch architecture consists of the processes and components used to effectively manage batch processing. The purpose of the batch architecture is to optimize processing (improve response time and utilization of system resources) by executing batch runs during off-peak periods. The architecture should provide the capacity manager with an easy to use interface and permit a standard and centralized approach to batch scheduling, monitoring, control, and error correction. The architecture should be highly scalable in order to meet the future needs of the organization. It should also be highly available, with minimal downtime, and minimize impact to online operations, which usually are operating concurrently with the batch operations. Some organizations may decide to have backup components, such as the event server, to ensure the completion of all mission-critical batch jobs.

The basic components of the batch architecture include the management server, capacity database (CDB), monitor, printer, application servers, and databases. In addition to the monitor attached to the management server, each application server should have a monitor to permit viewing of local batch-processing activity; this also facilitates error analysis at the local level.

### Batch Processing

Before discussing scheduled batch runs, it is useful to first understand the hierarchy of the batch process and the contents of a batch script. A batch run consists of multiple independent batch jobs that are scheduled for execution on a recurring basis. A large organization may execute multiple batch runs throughout the day, depending on the resources required to process them. Each batch job consists of multiple batch job steps that control specific activities of job execution.

An organization typically processes numerous batch jobs. To ensure a consistent approach to the execution of each job, a batch job skeleton should be devised that contains the standardized code required for each job; job-specific information should be coded into a designated area within the skeleton. The skeleton also serves to facilitate development and maintenance requirements by standardizing the content and structure of each job script. For example, any type of standardized actions, such as the notification of a successful or non-successful batch job execution and transaction data archiving and deletion, should be included in the code of every script that is executed.

Scheduled batch runs are initiated by a scheduling tool during a pre-defined batch window, typically when user activity of the system is at a minimum. After the scheduling tool has been programmed, capacity manager interaction should not be necessary during batch runs unless an error, from which the tool cannot recover, occurs.

The scheduling tool initiates all batch runs. If the run does not begin as scheduled, the tool halts the run and records an error in the error log; some scheduling tools may have the ability to attempt to restart the batch run. If the initialization is successful, the first batch job is executed. The scheduler manages the execution of jobs on each application server targeted to perform the batch processing. If no errors are encountered during the execution of the job run, then the tool records the successful completion of the job in the batch log and the next job is executed, and so on.

If an error occurs during the execution of a batch job, the scheduling tool stops processing that job and an error is sent to the error log. The actual execution of a batch job is dependent on a number of inputs that could be the reason that a job is not executed. For example, the following inputs may be required:

* Availability of production data
* Completion of a job on which the queued job is dependent
* Availability of resources to execute the job
* Priority of the job and the batch window

Warnings may also be generated during job processing if, for example, CPU or disk space capacity exceeds the threshold value for an application server processing the batch job. Warnings should not stop a batch job from being completed; however, the capacity manager should address all warnings as soon as possible because they may lead to future job processing failures. If an error causes a job to be stopped, some scheduling tools attempt to automatically recover from the problem and begin processing the job from the beginning of the job step that was executing when processing was stopped. Recovery is useful when processing very long batch jobs because jobs that are interrupted do not have to be restarted from the beginning. If recovery is not possible, the job needs to be restarted.

If the scheduling tool is not capable of restarting or recovering from a failed job (or able to restart or recover in a specific instance), the capacity manager has to manually initiate restart or recovery procedures.

### Job Scheduling Activities

Ideally, the batch architecture should be configured in such a manner that capacity manager interaction is kept to a minimum. However, there are still many daily tasks that the capacity manager must perform, including:

* Monitoring
* Analysis
* Tuning
* Implementation
* Event management
* As-needed request handling
* Schedule changing
* System backup
* Archiving
* Auditing
* Capacity manager log entry
* Reporting

Each of these activities is an integral part of the job scheduling process. The monitoring, analysis, tuning, and implementation activities form an iterative process. Inputs to the process include resource utilization and OLA thresholds against which the batch architecture is monitored. These are ongoing activities whose goal is to optimize the performance and utilization of the architecture. The remaining activities are performed in response to an event, request, or requirement.

### Documentation and Training

All policies and procedures should be clearly documented so that the capacity manager has a reference to refer to for daily operational guidance. Documentation should include information on:

* Procedures for starting and stopping batch runs.
* Procedures for changing job priority.
* Procedures for handling alerts and errors.
* Procedures for handling common errors.
* Procedures for analyzing the cause of errors.
* Procedures for escalating errors.
* Procedures for submitting RFCs.
* Procedures for documenting tasks in the capacity manager's log.
* Procedures for what should be monitored and when.
* Procedures for handling as-needed requests including reviewing, testing, and running these requests.

Without proper training, the capacity manager will not have the ability to conduct the activities discussed in this document. It is important that the capacity manager be properly trained so that processing errors can be responded to and corrected in a timely manner. If it is available, the capacity manager should attend vendor training on the scheduling tool utilized by the organization.

## Further Information

For more information, visit the [Microsoft Operations Framework](http://www.microsoft.com/mof) Web site.

To see how Microsoft IT uses Microsoft Operations Framework and best practice IT Service Management, go to <http://www.microsoft.com/technet/itshowcase/content/mofmmppt.mspx>.

## Checkpoint: Operating, Optimizing, and Change Processes

|  |  |
| --- | --- |
| X | Requirement |
|  | Implemented service level management across IT operations. |
|  | Implemented best practice release management. |
|  | Optimized network and system administration processes. |
|  | Implemented best practice job scheduling. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Rationalized level for Operating, Optimizing, and Change Processes of the Core Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for operations management in [Microsoft Operations Framework](http://www.microsoft.com/mof).

Additional Resources: Tools and Technologies

The following table lists the recommended tools, technologies, and services for moving from Standardized to Rationalized level.

| Name | Description |
| --- | --- |
| [Active Directory](http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx) | A central component of the Windows platform, Active Directory directory service provides the means to manage the identities and relationships that make up network environments. |
| [ActiveSync](http://www.microsoft.com/windowsmobile/activesync/default.mspx) | Microsoft ActiveSync provides support synchronization with Windows-based desktop computers and Microsoft Exchange Server. |
| [Antivirus Software](http://www.microsoft.com/athome/security/viruses/wsc/en-us/flist.mspx) | Antivirus software is specifically designed to detect and prevent viruses. |
| [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) | The Microsoft Application Compatibility Toolkit (ACT) is a life-cycle management tool that assists in identifying and managing your overall application portfolio and help resolve application compatibility issues. |
| [Business Desktop Deployment 2007 (BDD 2007)](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx) | A solution accelerator from Microsoft that provides comprehensive guidance and tools to manage large-scale desktop deployment projects, ongoing image management, and new-user desktop provisioning. |
| [Centralized Firewall Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/firewallservices/default.mspx) | Firewalls are software- or hardware-based devices that can be deployed between networks to protect an organization from external or internal network attacks. |
| [Group Policy](http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.mspx) | Group Policy is an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. |

|  |  |
| --- | --- |
| Name | Description |
| [Internet Authentication Service (IAS) and Remote Authentication Dial-In User Service (RADIUS)](http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/wificomp.mspx) | IAS in Windows Server 2003 or Network Policy Server (NPS) in the future with Windows Server “Longhorn” are Microsoft implementations of a RADIUS server and proxy. RADIUS is a client/server protocol where RADIUS clients send authentication and accounting requests to a RADIUS server. The RADIUS server checks the remote access authentication credentials on the user accounts and logs remote access accounting events. |
| [Microsoft Exchange Server](http://www.microsoft.com/technet/prodtechnol/exchange/default.mspx) | Messaging and collaboration software that enables users to send and receive e-mail and other forms of interactive communication through computer networks. |
| [Microsoft Office](http://www.microsoft.com/technet/prodtechnol/office/default.mspx) | Microsoft Office is a set of desktop productivity programs—including applications for word processing, e-mail, and spreadsheets—that integrate with servers, services, and solutions in the Microsoft Office system. |
| [Microsoft Operations Manager (MOM)](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx) | Provides comprehensive event and performance management, proactive monitoring and alerting, reporting and trend analysis, and system and application-specific knowledge and tasks to improve the manageability of Windows-based servers and applications. |
| [Networking Services](http://www.microsoft.com/technet/solutionaccelerators/wssra/raguide/networkservices/default.mspx) | Networking services are comprised of Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and Windows Internet Name Service (WINS). |
| [Microsoft Systems Management Server (SMS)](http://www.microsoft.com/technet/sms/default.mspx) | SMS is a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to quickly and cost-effectively provide relevant software and updates to users from Microsoft and non-Microsoft vendors. |
| [SMS 2003 Desired Configuration Monitoring](http://www.microsoft.com/downloads/details.aspx?FamilyID=a867fc14-daa3-4c2a-9e65-4fbcbec60aaa&DisplayLang=en) | SMS 2003 Desired Configuration Monitoring enables you to define customized configuration standards for desktops and servers and then perform automated compliance audits against defined configuration standards. |
| [System Center Operations Manager](http://www.microsoft.com/technet/opsmgr/default.mspx) |  |

|  |  |
| --- | --- |
| Name | Description |
| [System Center Configuration Manager](http://www.microsoft.com/technet/sms/default.mspx) | System Center Configuration Manager 2007 provides a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to provide relevant software and updates to users quickly and cost-effectively. |
| [System Center Operations Manager](http://www.microsoft.com/technet/opsmgr/default.mspx) | System Center Operations Manager 2007 is the next version of Microsoft’s event and performance monitoring solution, Microsoft Operations Manager. Operations Manager 2007 improves on the functionality of its predecessor by extending monitoring to IT Services and desktop clients. |
| [Windows Automated Installation Kit (Windows AIK)](http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&) | The Windows Automated Installation Kit (Windows AIK) is designed to help Original Equipment Manufacturers (OEMs), system builders, and IT professionals deploy Windows onto new hardware. |
| [Windows Mobile](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx) | Windows Mobile is software for mobile devices to enable sending and receiving e-mail, browsing the Internet, and mobile use of Office productivity software. |
| [Windows Server](http://www.microsoft.com/technet/windowsserver/default.mspx) 2003 | Windows Server 2003 is an infrastructure platform for powering connected applications, networks, and Web services from the workgroup to the data center. |
| [Windows Server Update Services (WSUS)](http://technet2.microsoft.com/windowsserver/en/technologies/featured/wsus/default.mspx) | Enables IT administrators to deploy many of the latest Microsoft product updates published to the Microsoft Update site. |
| [Windows Vista](http://www.microsoft.com/windows/products/windowsvista/default.mspx) | Windows Vista is the latest desktop operating system from Microsoft. Feature improvements have been made to deployment and management, desktop search, mobility, and security. |
| [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625) | Windows Vista Hardware Assessment is an agentless tool that makes it easier for customers and consultants to inventory and assess their PCs' hardware and device driver compatibility network-wide in preparation for Windows Vista migration. |

# 

Additional Resources: Standardized to Rationalized Checklist

The following checklist outlines the requirements you must meet to move to the Rationalized level. After you have addressed each item under the main topics, you have successfully moved from the Standardized level to the Rationalized level.

## Capability: Identity and Access Management

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops** |  |  |
| Attributes:   * Identified which configurations should be monitored or enforced. * Selected tools for monitoring and enforcing configuration compliance. * Defined Group Policy objects for settings managed through Group Policy. * Implemented Group Policy Management Console to manage Group Policy objects. * Applied Group Policy to at least 80 percent of your desktops. | | |

## Capability: Desktop, Device and Server Management

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **An automated software distribution solution for operating system deployment** |  |  |
| Attributes:   * Identified tools and technologies required to enable automated operating system deployment. * Performed necessary pre-deployment tasks for application compatibility and packaging, infrastructure remediation, imaging, user-state migration, and desktop security. * Tested and validated Zero Touch Installation in a lab environment and pilot program. * Performed automated OS deployment to end users. | | |

|  |  |  |
| --- | --- | --- |
| Requirement 2 | Yes | No |
| **Automated tracking of hardware and software assets of 80 percent or more of your desktops** |  |  |
| Attributes:   * Deployed tools and procedures to automate desktop asset inventory. * Implemented procedures and technologies to automate application and operating system deployment * Implemented tools and procedures to perform and analyze software usage tracking reporting. * Implemented best practice automated software update management. * Deployed tools and procedures to monitor desktop system status, including product compliance and system status monitoring. | | |
| Requirement 3 | Yes | No |
| **Eighty percent or more of your desktops running one of the two most recent operating system versions** |  |  |
| Attributes:   * Inventoried existing production operating systems. * Determined new computer and refresh strategies in order to phase out older operating systems. * Deployed two most recent operating system versions to at least 80 percent of all desktops. | | |
| Requirement 4 | Yes | No |
| **Eighty percent or more of your desktops running Microsoft Office 2003 or the 2007 Microsoft Office system** |  |  |
| Attributes:   * Evaluated the latest versions of Office and defined plan to consolidate Office versions on production workstations. * Deployed latest versions of Office to desktops. * Defined plan for managing Office configurations. | | |
| Requirement 5 | Yes | No |
| **Tests and certifies application compatibility on 80 percent of new or updated applications before deploying them to desktops** |  |  |
| Attributes:   * Collected and analyzed the application inventory in your organization to build your application portfolio. * Implemented standard testing of your mitigation strategies to create your application mitigation packages. * Implemented standard processes to resolve any outstanding compatibility issues to report compatibility mitigation to management. * Implemented automated deployment of all compatibility mitigation packages. | | |
| Requirement 6 | Yes | No |
| **Patch management solution for 80 percent or more of your servers** |  |  |
| Attributes:   * Implemented process and tools to inventory hardware and software assets. * Implemented process and tools to scan servers for software updates. * Established a process to automatically identify available patches. * Established standard testing for every patch. * Implemented patch distribution software. | | |
| Requirement 7 | Yes | No |
| **Secured and guaranteed way to verify secure communications between your corporate network and mobile devices** |  |  |
| Attributes:   * Inventoried mobile devices connecting to your network. * Determined a communication security strategy appropriate for your needs. * Implemented mobile device authentication to all connected devices. | | |
| Requirement 8 | Yes | No |
| **Access provided to Web applications via WAP or HTTP for mobile devices** |  |  |
| Attributes:   * Inventoried mobile devices connecting to your network and Web applications currently consumed or potentially consumed by mobile device users. * Developed and implemented a strategy to optimize Web applications for mobile device users, update mobile device hardware, or both. | | |
| Requirement 9 | Yes | No |
| **Planning for server consolidation with virtualization** |  |  |
| Attributes:   * Inventoried all IT services and LOB applications in your organization, including performance and traffic data. * Developed a plan to consolidate server infrastructure by implementing virtual machine technologies. | | |
| Requirement 10 | Yes | No |
| **Implemented a layered-image strategy for managing your desktop images** |  |  |
| Attributes:   * Inventoried and rationalized the current set of managed desktop images in your organization. * Developed and implemented a strategy to consolidate desktop images by using thin or hybrid layered-imaging for desktop deployment. | | |

## Capability: Security and Networking

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Policy-managed firewall on 80 percent or more of your servers and desktops** |  |  |
| Attributes:   * Inventoried your desktop and server computers to identify which hardware currently has host-based firewall technologies. * Deployed host-based firewall technology to hardware lacking firewall capabilities or updated servers to Windows Server 2003 SP1 or later. * Established policy enforcement to ensure host-based firewalls are always enabled and cannot be disabled. | | |
| Requirement 2 | Yes | No |
| **Secure remote access to internal resources and line-of-business applications beyond e-mail (that is, VPN and/or Terminal Services)** |  |  |
| Attributes:   * Evaluated remote access requirements for remote clients and branch offices. * Designed and implemented secure virtual private network or similar services to remote clients and branch office. | | |
| Requirement 3 | Yes | No |
| **Secured and guaranteed way to verify communication between critical servers, such as domain controllers and e-mail servers** |  |  |
| Attributes:   * Assessed the current state of network infrastructure affected by Internet Protocol Security (IPsec). * Identified organizational requirements to ensure secured and guaranteed communication between servers, including regulation and compliance impacts. * Developed and implemented a plan across the organization using IPsec to meet defined requirements. | | |
| Requirement 4 | Yes | No |
| **Monitoring and service level reporting for 80 percent or more of your servers to ensure a consistent and reliable user experience** |  |  |
| Attributes:   * Defined your organization’s IT services in a service catalog. * Determined the baseline or current service levels for defined services. * Defined service levels appropriate for your organization and determined a plan for automating service level monitoring. * Implemented an automated availability monitoring solution. | | |

|  |  |  |
| --- | --- | --- |
| Requirement 5 | Yes | No |
| **Providing a secured communication mechanism for presence** |  |  |
| Attributes:   * Assessed any current unmanaged methods used for presence and instant communication. * Created a requirements specification for presence and instant messaging, aligning to industry or local regulations and policies. * Evaluated presence and instant technology and created a plan to implement your selected solution. * Implemented presence at minimum through managed instant messaging and optionally through collaboration and e-mail infrastructure. | | |
| Requirement 6 | Yes | No |
| **Deployed a secure wireless network using Active Directory and IAS/RADIUS for authentication and authorization** |  |  |
| Attributes:   * Identified current wireless access and related topologies. * Evaluated wireless technologies, protocols, and standards. * Developed and implemented plans for secure wireless authentication infrastructure. | | |
| Requirement 7 | Yes | No |
| **Centrally managed certificate services infrastructure (PKI)** |  |  |
| Attributes:   * Performed a network discovery to inventory all components. * Identified people, process and technology design considerations for the certification authority and public key infrastructure. * Created a detailed deployment plan to enable the PKI. * Implemented PKI deployment plan. | | |
| Requirement 8 | Yes | No |
| **Proactively managing bandwidth to branch offices** |  |  |
| Attributes:   * Identified and documented branch office topology. * Created requirement specification based on the needs of all branch office types. * Created a plan and architecture for branch office service consolidation and identified performance thresholds for reexamination of branch office WAN requirements. * Implemented plan to optimize branch office services against WAN link limitations. | | |

## Capability: Data Protection and Recovery

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Centrally managing data backup for your branch offices** |  |  |
| Attributes:   * Created a centralized data backup plan and a recovery plan for branch offices in your organization. * Implemented a backup and recovery plan for centralized control of backup and recovery operations, either via network-centralized tools or operational guidelines for local backup and recovery, with defined service levels. | | |
| Requirement 2 | Yes | No |
| **Service level agreement (SLA) for system backup and restore, and defined recovery times for 80 percent of your servers** |  |  |
| Attributes:   * Created a data backup plan and a recovery plan for 80 percent or more of all servers in your organization. * Used drills to test your plans and validate defined recovery times. | | |

### Capability: Security and ITIL/COBIT-based Management Process

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Established security processes for two-factor user authentication, standard security review for new software acquisitions, and data classification** |  |  |
| Attributes:   * Developed and implemented two-factor identity and access management policies. * Developed a process to manage security requirement testing on all acquired or developed software. * Established a standard and repeatable procedure for classifying sensitive data. | | |
| Requirement 2 | Yes | No |
| **Implemented best practices for operating, optimizing, and change processes in your IT organization** |  |  |
| Attributes:   * Implemented service level management across IT operations. * Implemented best practice release management. * Optimized network and system administration processes. * Implemented best practice job scheduling. | | |