

Core Infrastructure Optimization   
Implementer Resource Guide:   
Basic to Standardized

Published: February 2007

Updated: August 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. With each level of optimization, the IT infrastructure also brings about significant cost reduction, increased security, and improved availability and manageability.

This is the first 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 Basic level to the Standardized 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>.

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

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT.

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

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

© 2007 Microsoft Corporation. All rights reserved. This work is licensed 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.

Microsoft, Active Directory, ActiveSync, SharePoint, Windows, Windows Mobile, Windows NT, Windows Server, and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All other trademarks are property of their respective owners.

Contents

[Core Infrastructure Optimization Implementer Resource Guide: Basic to Standardized 1](#_Toc180213830)

[Resource Guide Overview 1](#_Toc180213831)

[Audience 1](#_Toc180213832)

[Infrastructure Optimization Concept 1](#_Toc180213833)

[Core Infrastructure Optimization Capabilities 3](#_Toc180213834)

[Core Infrastructure Optimization Model Levels 3](#_Toc180213835)

[Capability: Identity and Access Management 13](#_Toc180213836)

[Introduction 13](#_Toc180213837)

[Requirement: Directory Services for Authentication of Users 14](#_Toc180213838)

[Capability: Desktop, Device and Server Management 19](#_Toc180213839)

[Introduction 19](#_Toc180213840)

[Requirement: Automated Patch Distribution to Desktops and Laptops 20](#_Toc180213841)

[*Checkpoint: Automated Patch* *Distribution to Desktops and Laptops* 24](#_Toc180213842)

[Requirement: Defined Standard Images for Desktops and Laptops 25](#_Toc180213843)

[*Checkpoint: Defined Standard Images for Desktops and Laptops* 29](#_Toc180213844)

[Requirement: Centralized Management of Mobile Devices 29](#_Toc180213845)

[*Checkpoint: Centralized Management of Mobile Devices* 34](#_Toc180213846)

[Requirement: Identity Validation, Data Protection, and Data Backup of Mobile Devices 34](#_Toc180213847)

[*Checkpoint: Identity Validation, Data Protection, and Data Backup of Mobile Devices Checkpoint* 37](#_Toc180213848)

[Requirement: Consolidation of Desktop Images to Two Operating System Versions 37](#_Toc180213849)

[*Checkpoint: Consolidation of Desktop Images to Two Operating System Versions* 39](#_Toc180213850)

[Capability: Security and Networking 41](#_Toc180213851)

[Introduction 41](#_Toc180213852)

[Requirement: Antivirus Software for Desktops 42](#_Toc180213853)

[*Checkpoint: Antivirus Software for Desktops* 45](#_Toc180213854)

[Requirement: Centralized Firewall Services 45](#_Toc180213855)

[*Checkpoint: Centralized Firewall Services* 49](#_Toc180213856)

[Requirement: Internally Managed Basic Networking Services (DNS, DHCP, WINS) 49](#_Toc180213857)

[*Checkpoint: Internally Managed Basic Networking Services (DNS, DHCP, WINS)* 52](#_Toc180213858)

[Requirement: Availability Monitoring of Critical Servers 53](#_Toc180213859)

[*Checkpoint: Availability Monitoring of Critical Servers* 56](#_Toc180213860)

[Capability: Data Protection and Recovery 57](#_Toc180213861)

[Introduction 57](#_Toc180213862)

[Requirement: Defined Backup and Restore Services for Critical Servers 58](#_Toc180213863)

[*Checkpoint: Defined Backup and Restore Services for Critical Servers* 62](#_Toc180213864)

[Capability: Security Process 63](#_Toc180213865)

[Introduction 63](#_Toc180213866)

[Requirement: Security Policies, Risk Assessment, Incident Response, and Data Security 64](#_Toc180213867)

[*Checkpoint: Security Policies, Risk Assessment, Incident Response, and Data Security* 67](#_Toc180213868)

[Capability: ITIL/COBIT-Based Management Process 69](#_Toc180213869)

[Introduction 69](#_Toc180213870)

[Requirement: Support and Change Management Process 70](#_Toc180213871)

[*Checkpoint: Support and Change Management Process* 77](#_Toc180213872)

[Additional Resources: Tools and Technologies 79](#_Toc180213873)

[Additional Resources: Basic to Standardized Checklist 81](#_Toc180213874)

Core Infrastructure Optimization   
Implementer Resource Guide:   
Basic to Standardized

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 Basic level to the Standardized 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 |
| Data Protection and Recovery |
| Security and Networking |
| 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 infrastructure 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 Basic level of IT infrastructure and processes to the Standardized 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, solutions that should be implemented 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.

## 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.

## Security and Networking

Describes what customers should consider implementing in their IT infrastructure 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.

## 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 as follows:

## 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

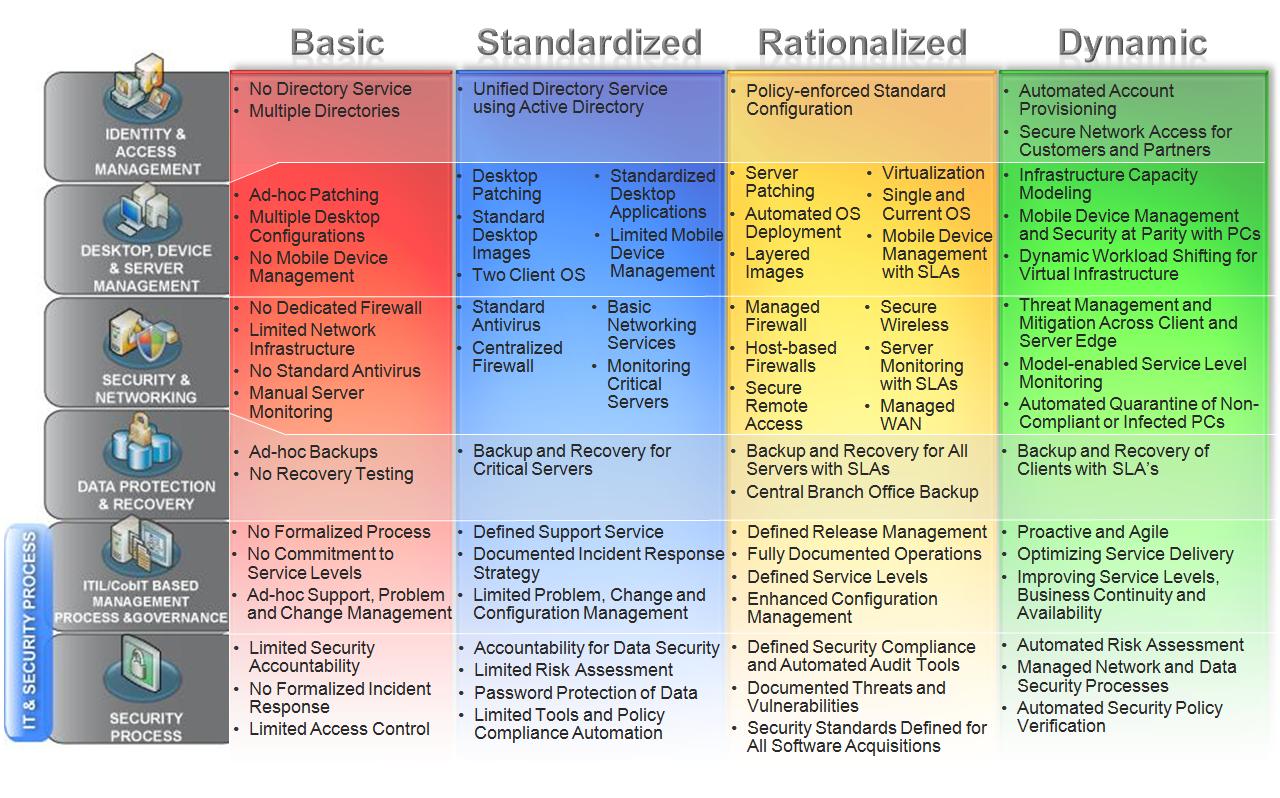
The Rationalized infrastructure is where the costs involved in managing desktops and servers are at their lowest and processes and policies have been optimized to begin playing a large role in supporting and expanding the business. Security is very proactive and responding to threats and challenges is 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, 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.



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 answer 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 Standardized level and can proceed to the Rationalized 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 Standardized level of optimization requires that an Active Directory directory service be in place in your organization and is used to authenticate 80 percent or more of your users.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented Active Directory directory service for authentication of 80 percent or more of connected users |  |  |

For more details, see [Directory Services for Authentication of Users](#DSDOC_BKMK_TOOLS88f80cb7_d44f_47f7_a10d_) 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)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx)
* [Microsoft Operations Framework Directory Services Administration](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfdirsa.mspx)

### Capability: Desktop, Device and Server Management

The Standardized level of optimization requires that your organization has procedures and tools in place to automate patch distribution, manage and consolidate standard desktop images, and centrally manage connected mobile devices.

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Automated patch distribution covering 80 percent or more of your desktops |  |  |
| Attributes:   * 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. | | |

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

* [Microsoft TechNet Update Management Center](http://www.microsoft.com/technet/updatemanagement/default.mspx)
* [Microsoft Systems Management Server (SMS)](http://www.microsoft.com/technet/updatemanagement/plan/sms-step1.mspx)
* [Patch Management using SMS 2003 Solution Accelerator](http://www.microsoft.com/downloads/details.aspx?FamilyId=E9EAB1BD-13E7-4E25-85C5-CE2D191C3D63&displaylang=en)
* [Microsoft Windows Server® Update Services (WSUS)](http://technet2.microsoft.com/WindowsServer/en/library/d446d310-413f-4844-8aad-c557712397401033.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| A defined set of standard, basic images for 80 percent or more of your desktops and laptops |  |  |
| Attributes:   * Defined a strategy for standard images. * Used tools to capture a standard image. * Defined a standard set of disk images (OS and applications) for all hardware types. * Established deployment tools for network-based or offline image installation. | | |

For more details, see [Standardized Computer Images](#_Standardized_Computer_Images) in this document, or visit the following Web sites:

* [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx)
* [BDD 2007 Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| A centralized solution to track, manage, and upgrade your mobile devices |  |  |
| Attributes:   * Installed software to discover and track the mobile devices in your organization. * Implemented password-controlled access. * Established centralized data and software synchronization. * Ensured that decommissioned devices are free of company information. | | |

For more details, see [Centralized Management of Mobile Devices](#_Consolidation_of_Desktop) in this document, or visit the following Web sites:

* [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx)
* [Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2](http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx)
* [Microsoft TechNet Exchange Server TechCenter](http://www.microsoft.com/technet/prodtechnol/exchange/default.mspx)
* [Systems Management Server 2003 Device Management Feature Pack (DMFP)](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/downloads/featurepacks/dmfp.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| A solution for user identity validation and data protection, if lost, for your mobile devices |  |  |
| Attributes:   * Established and are enforcing a password-access policy or using public key certificates for user identification. * Encrypted all transfers for data distribution to, and data backup from, mobile devices. * Implemented device lockout on mobile devices. * Ensured that company information can be removed with remote wipe in case a mobile device is lost or stolen. | | |

For more details, see [Identity Validation, Data Protection, and Data Backup of Mobile Devices](#_Identity_Validation,_Data) in this document, or visit the following Web sites:

* [Microsoft TechNet Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx)
* [Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2](http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx)
* [Microsoft TechNet Exchange Server TechCenter](http://www.microsoft.com/technet/prodtechnol/exchange/default.mspx)
* [Systems Management Server 2003 Device Management Feature Pack (DMFP)](http://www.microsoft.com/technet/downloads/sms/2003/featurepacks/dmfp.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| A maximum of two operating system versions on 80 percent of your desktops |  |  |
| Attributes:   * Implemented an image-consolidation strategy. * Reduced the number of production operating systems to no more than two. | | |

For more details, see [Consolidation of Desktop Images to Two Operating System Versions](#_Consolidation_of_Desktop_1) in this document, or visit the following Web sites:

* [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx)
* [BDD 2007 Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx)

### Capability: Security and Networking

The Standardized 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 |
| Antivirus software (with automated signature updating) running on 80 percent or more your desktops |  |  |
| Attributes:   * Installed all operating system and software application security updates. * Enabled available host-based firewalls. * Installed antivirus software on eighty percent or more of your desktop computers. | | |

For more details, see [Antivirus Software for Desktops](#_Antivirus_Software_for) in this document, or visit the following Web site:

[The Antivirus Defense-in-Depth Guide](http://www.microsoft.com/technet/security/guidance/serversecurity/avdind_0.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Firewall (not per desktop) for your organization protecting 80 percent or more of your systems |  |  |

For more details, see [Centralized Firewall Services](#_Centralized_Firewall_Services) in this document, or visit the following Web sites:

* [Windows Server System Reference Architecture Firewall Services Implementation Guide](http://www.microsoft.com/technet/itsolutions/wssra/raguide/firewallservices/default.mspx)
* [Microsoft TechNet Internet Security and Acceleration Server TechCenter](http://www.microsoft.com/technet/isa/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Internal servers for basic networking services (DNS, DHCP, WINS) |  |  |
| Attributes:   * Implemented DNS services on servers or other devices within your organization. * Implemented DHCP services on servers or other devices within your organization. * Implemented WINS services for older operating systems on servers or other devices within your organization. | | |

For more details, see [Internally Managed Basic Networking Services (DNS, DHCP, WINS)](#_Internally_Managed_Basic) in this document, or visit the following Web sites:

* [Windows Server System Reference Architecture Introduction to Network Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/networkservices/default.mspx)
* [Windows Server 2003 Deployment Guide](http://technet2.microsoft.com/WindowsServer/en/library/c283b699-6124-4c3a-87ef-865443d7ea4b1033.mspx)
* [Microsoft TechNet Windows Server TechCenter](http://www.microsoft.com/technet/windowsserver/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Monitoring for 80 percent or more of your critical servers to ensure a consistent and reliable user experience |  |  |
| Attributes:   * Installed availability monitoring software such as Microsoft Operations Manager (MOM). * Are monitoring 80 percent of your critical servers for performance, events, and alerts. | | |

For more details, see [Availability Monitoring of Critical Servers](#_Availability_Monitoring_of) 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 TechNet Operations Manager 2005 TechCenter](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx)

### Capability: Data Protection and Recovery

The Standardized level of optimization requires that your organization has procedures and tools in place to manage backup and recovery of data on critical servers.

|  |  |  |
| --- | --- | --- |
| Requirement: Data Protection and Recovery | Yes | No |
| Backup and restore solution for 80 percent or more of your business-critical servers |  |  |
| Attributes:   * Created a data backup plan and a recovery plan for eighty percent or more of your critical servers. * Used drills to test your plans. | | |

For more details, see [Defined Backup and Restore Services for Critical Servers](#_Defined_Backup_and_2) 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 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 Standardized 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 |
| Risk assessment methodology and incident response plan, consistent security policy compliance, and evaluation and testing of all acquired software |  |  |
| Attributes:   * Named a dedicated person for security strategy and policy. * Established a risk assessment methodology. * Established an incident response plan. * Established a process to manage user, device, and service identities. * Established consistent processes to identify security issues, including all network-connected devices. * Established consistent security policy compliance on network devices. * Established a plan to evaluate and test all acquired software for security compliance. * Established a consistent policy to classify data. | | |

For more details, see [Security Policies, Risk Assessment, Incident Response, and Data Security](#_Security_Policies,_Risk_1) in this document, or visit the following Web site:

[Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and ITIL/COBIT-Based Management Process | Yes | No |
| A defined process for problem, incident, service, configuration, and change management |  |  |
| Attributes:   * Implemented Problem Management techniques. * Implement Incident Management techniques. * Improved end-user support services. * Implemented Change Management best practices. | | |

For more details, see [Support and Change Management Process](#_Support_and_Change) 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)

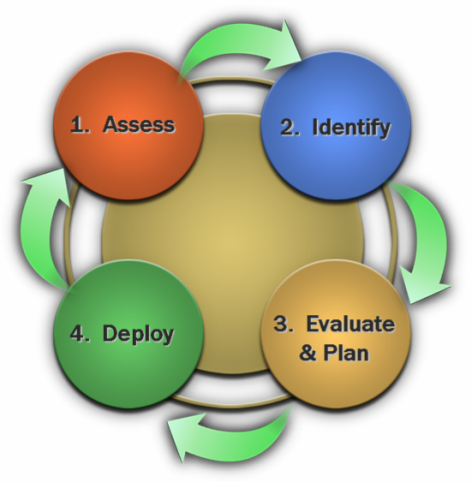
## Preparing to Implement Core IO Requirements

The detailed capability and requirement sections of the Core Infrastructure Optimization Implementer Resource Guide: Basic to Standardized 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 Standardized 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.



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: Basic to Standardized 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 in 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 Standardized level in Identity and Access Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Users continually receive authentication prompts, have trouble logging in  Too many user identity stores to manage  No consistency in accessing resources  Risk of unauthorized access to confidential information  Difficulty implementing compliance with governmental regulations (Sarbanes – Sarbanes-Oxley, HIPAA, etc.)  Newly hired workers must wait to access crucial systems, reducing productivity  **IT Challenges**  Rising help desk costs associated with password resets and access requests  Lack of centrally managed identities, no clear view of identity life cycle  Orphan accounts pose a security risk  Identities vary across systems, no central repository for identities | **Projects**  Implement primary directory service for client authentication  Implement directory service–aware clients | **Business Benefits**  Increased user productivity through simplified logon process  Lower administration costs due to management of fewer identity stores  Progressing toward implementing compliance with regulations  Reduced cost of managing user accounts  **IT Benefits**  Reduced helpdesk volume  Fewer digital identities  Identities are centrally managed  Improved security |

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/p2prov.mspx)
* Access Management and Single Sign On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P3Intran.mspx)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P3Extran.mspx)

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).

In the Infrastructure Optimization Model, the Standardized level of Identity and Access Management addresses the need for directory services for authentication of users and requires a unified directory service for authentication of at least 80% of users. Conversely, this requirement implies that all clients are aware of the directory service.

# Requirement: Directory Services for Authentication of Users

## Audience

The Standardized level of optimization requires that an Active Directory directory service be in place in your organization and is used to authenticate 80 percent or more of your users. You should read this section if you do not use Active Directory for authentication of 80 percent or more of your users.

## Overview

User authentication is required for many reasons during the course of a user’s workday. Network access, application access, data access, and e-mail access are typical examples. When you enable directory services for user authentication you centralize and unify all these separate authentication requirements. A single logon then gives the user access to all resources, applications, and data that the user is authorized to access.

## Phase 1: Assess

The Assess phase primarily takes inventory of which directory services, if any, are used in your organization. You will define the reasons for each directory service and how they are used. If your organization does not have a directory service in place, you will need to examine how identities are currently managed and what processes are in place to secure access to data resources; these can be formal/documented or informal/undocumented processes.

## Phase 2: Identify

The directory service design process begins by identifying the technologies available to provide the service and what your organization’s needs are in the implementation of a directory service.

An Active Directory infrastructure is required by the Core Infrastructure Optimization Model and provides foundational support for many services required by the organization, including messaging and collaboration, systems management, and security services. Active Directory is the network-focused directory service included in Microsoft® Windows® 2000 and Windows Server® 2003.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase leads you through the planning and design process for to meet your organizations needs. It is imperative that you manage information relating to employees and their use of computing resources with a single, coherent authentication system, one that possesses the characteristics required for the most efficient management of this information.

It should be organized and presented as a directory.

A common method of querying should be supported, regardless of the type of data being requested.

Information with similar characteristics should be managed in a similar manner.

The ways in which information is grouped and managed should be determined by the organization, in ways that complement the organization's existing systems.

### Designing the Directory Service

When designing the service, five categories of directories are used:

* Specific-use d.irectories
* Application directories
* Network-focused directories
* General-purpose directories
* Metadirectories

An Active Directory administrator has complete control over how information is presented in the directory. The information can be grouped into containers called organizational units (OUs) that are often arranged to facilitate the hierarchical storage of data. The types of data stored in the directory are defined using a schema specifying classes of data called *objects*. A user object, for example, is the User class defined in the schema. Attributes of the user object store information; for example, user name, password, and telephone number. The administrator can update the schema to include new attributes or classes as required.

For more information on defining the Active Directory directory service, go to <http://www.microsoft.com/technet/itsolutions/wssra/raguide/DirectoryServices/igdrbp_2.mspx#E4F>.

### Designing the Active Directory Structure

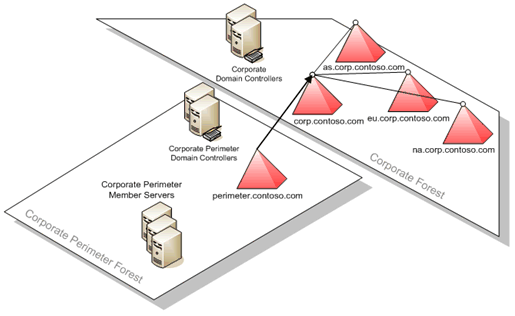
The logical structure of Active Directory can be considered as a number of logical directories called domains. The collection of domains is called a forest because directory data in each domain is typically organized in a tree-like structure to reflect the organization.

The process for designing the logical structure consists of the following steps:

1. **Logical Structure Design Requirements**. The Active Directory functions for administrative delegation are central to the logical structure design. Administration of specific OUs can be delegated to achieve autonomy or isolation of a service or data. Administrative delegation is done to meet the legal, operational, and organizational structure requirements.
2. **Forest Design**. A forest design model is chosen after the appropriate number of forests is determined in the service design process; for example, when multiple directories are necessary or object definitions vary within an organization. With few exceptions, we recommend that you maintain a single forest to be able to standardize the directory service.
3. **Domain Design**. A domain model is then chosen for each forest.
4. **Forest Root Design**. Forest root decisions are based on the domain design. If a single-domain model is chosen, the single domain functions as the forest root domain. If a regional-domain model is chosen, the forest owner needs to determine the forest root.
5. **Active Directory Namespace Planning**. After the domain model is determined for each forest, the namespace for the forest and domains should be defined.
6. **DNS Infrastructure to Support Active Directory**. After the Active Directory forest and domain structures have been designed, the Dynamic Name System (DNS) infrastructure design for Active Directory can be completed.
7. **Creating an Organizational Unit Design**. OU structures are unique to the domain, not the forest, so each domain owner is responsible for designing the OU structure for their domain.

### Rendering the Logical Design

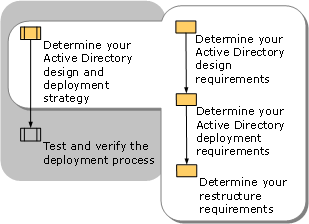
After the service design steps are completed, you can create a logical design that can be used to communicate the design to others, and to verify the integrity of the proposed design. This logical design should provide the required level of detail to allow the designers and IT professionals to understand the proposed design and to ensure that it meets the requirements of the services that they are responsible for within the overall enterprise design. The following diagram is an example of logical design. In the following example, the corporate forest uses a regional-domain model, which was chosen so that replication across the WAN could be carefully controlled.



For more information on designing the Active Directory logical structure, go to<http://www.microsoft.com/technet/itsolutions/wssra/raguide/DirectoryServices/igdrbp_2.mspx#EELAE>.

## Phase 4: Deploy

After you perform a high-level assessment of your current environment and determine your Active Directory deployment goals, you can determine the deployment strategy that works best for your environment. The following figure shows the steps for defining the Active Directory deployment process.



The Active Directory deployment strategy that you apply varies according to your existing network configuration. For example, if your organization currently runs Windows 2000, you can simply upgrade your operating system to Windows Server 2003. If your organization currently runs Microsoft Windows NT® 4.0 or a non-Windows network operating system, however, you must design an Active Directory infrastructure before you upgrade to Windows Server 2003.

Your deployment process might involve restructuring existing domains, either within an Active Directory forest or between Active Directory forests. You might need to restructure your existing domains after you deploy Windows Server 2003 Active Directory or after organizational changes or corporate acquisitions.

For more information on prerequisites for deploying the Active Directory infrastructure, go to <http://technet2.microsoft.com/WindowsServer/en/library/e0966784-1185-4b41-a259-68513689493b1033.mspx>.

## Operations

The goal of directory services is to ensure that information is accessible through the network by any authorized requester via a simple and organized process. The following resources provide information on operating Active Directory in your organization after it has been implemented and all objects are defined. Operating an Active Directory infrastructure requires proper administration of domain and forest trusts, Windows time service, SYSVOL, the global catalog, Active Directory backup and restore, intersite replication, the Active Directory database, and domain controllers.

For more information, visit:

* [Microsoft Operations Framework Directory Services Administration](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfdirsa.mspx)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx):
* [Administering Domain and Forest Trusts](http://technet2.microsoft.com/WindowsServer/en/library/03048bab-cc2b-4b49-ad8d-0a4d9ae2727f1033.mspx?mfr=true)
* [Administering the Windows Time Service](http://technet2.microsoft.com/WindowsServer/en/library/ac86e77c-0be3-430a-ba0b-c2225506fc4f1033.mspx?mfr=true)
* [Administering SYSVOL](http://technet2.microsoft.com/WindowsServer/en/library/59f1f1ca-5bb2-4d98-8856-473910b79cfe1033.mspx?mfr=true)
* [Administering the Global Catalog](http://technet2.microsoft.com/WindowsServer/en/library/a9346f44-af5f-41e5-9fc5-850b3b51f7361033.mspx?mfr=true)
* [Administering Operations Master Roles](http://technet2.microsoft.com/WindowsServer/en/library/c010993c-b7ff-439a-b45c-e15ba1312a931033.mspx)
* [Administering Active Directory Backup and Restore](http://technet2.microsoft.com/WindowsServer/en/library/f66ee9e4-96d7-4f74-a2fe-d669194bf5a21033.mspx?mfr=true)
* [Administering Intersite Replication](http://technet2.microsoft.com/WindowsServer/en/library/60ea064a-d867-4848-9baf-b1f7f9e368ff1033.mspx)
* [Administering the Active Directory Database](http://technet2.microsoft.com/WindowsServer/en/library/e6e282de-f4b3-4ea6-a231-37fb5ddffa1b1033.mspx)
* [Administering Domain Controllers](http://technet2.microsoft.com/WindowsServer/en/library/5174e71a-2a3d-4817-9014-bfaaca598a461033.mspx)
* The Technology Center for Active Directory in Windows Server 2003 contains information on implementing Active Directory in Windows Server 2003:

<http://www.microsoft.com/windowsserver2003/technologies/activedirectory/default.mspx>

* The Product and Technology Security Center for Active Directory and Kerberos is a consolidated list of resources that can be consulted for security updates and “how-to” guidance:

<http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/featured/ad/default.mspx>

* For information on Active Directory on the Microsoft Support Web site, visit <http://support.microsoft.com/default.aspx?scid=fh;EN-US;winsvr2003ad>.

### Further Information

For more information on directory services and authentication, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search on "Active Directory authentication."

For additional Active Directory product guidance, see

* [Planning an Active Directory Deployment Project](http://technet2.microsoft.com/WindowsServer/en/library/e0966784-1185-4b41-a259-68513689493b1033.mspx)
* [Designing the Active Directory Logical Structure](http://technet2.microsoft.com/WindowsServer/en/library/2bd36720-ed2e-47ed-a80d-fa43a403b4361033.mspx)

To see how Microsoft utilizes Active Directory, go to <http://www.microsoft.com/technet/itshowcase/content/managead.mspx>.

## Checkpoint: Directory Services for Authentication of Users

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented Active Directory directory service for authentication of 80 percent or more of connected users. |

If you have completed the step listed above, your organization has met the minimum requirement of the Standardized level for this capability based on the Infrastructure Optimization model. We recommend that you follow additional best practice resources for operating your Active Directory infrastructure after it has been deployed.

Go to the [next Self-Assessment question](#_Do_you_have).

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 Standardized level in Desktop, Device and Server Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Risk of unauthorized access to sensitive data on mobile devices  Inability to define mobile policies by organization or unit  Policies for device settings vary  Lack of centralized corporate standards for managing or enforcing device policies  **IT Challenges**  No standards for hardware, operating systems, and applications  Desktops are not centrally managed, resulting in increased operations and software distribution costs  Inconsistent patch management leads to more security vulnerabilities  IT is highly reactive, spending resources fighting unpredicted issues  Inability to remotely remove data from lost or stolen devices | **Projects**  Deploy automated, centralized patch management solution  Implement standardized lite touch, image-based deployment solution  Implement a management solution for monitoring critical servers  Implement a mobile device provisioning solution that includes security policy provisioning, remote wipe, and policy enforcement | **Business Benefits**  Mobile workers stay current with direct connectivity between corporate networks and devices  Using a system management tool will reduce per-PC management costs  **IT Benefits**  Monitoring services help simplify identification issues, quickly determine the cause of the problem, and efficiently restore services to prevent potential IT problems  PCs that are faster and less expensive to deploy  Reduced help desk and operations costs  Administrators can ensure data protection and compliance with corporate security policies, including ability to set password policies and remotely remove data from devices |

The Standardized level in the Infrastructure Optimization Model addresses the key areas of management including:

* Automated Patch Distribution to Desktops and Laptops
* Defined Standard Images for Desktops and Laptops
* Consolidation of Desktop Images to Two Operating System Versions
* Centralized Management of Mobile Devices
* Identity Validation, Data Protection, and Data Backup of Mobile Devices

The Standardized level of optimization requires that your organization has procedures and tools in place to automate patch distribution, manage and consolidate standard desktop images, and centrally manage connected mobile devices.

# Requirement: Automated Patch Distribution to Desktops and Laptops

## Audience

You should read this section if you do not have an automated patch distribution process in place for 80 percent or more of your desktops and laptops.

## Overview

IT professionals today face immense challenges in implementing an effective software update management strategy: more devices and mobile users are now accessing corporate networks; there is a consistent stream of security updates from software and hardware vendors; footprints for systems and applications are expanding; there is an almost daily identification of new security threats; and the hacking community is now much more sophisticated.

## Phase 1: Assess

The Assess phase is the first major step in the patch management process. The process starts with assessment, because you will need to determine what you have in your production environment, the security threats and vulnerabilities you might face, and whether your organization is prepared to respond to a new operating system or application software update.

Ideally, assessment is an ongoing process that you should follow to ensure that you always know what computing assets you have, how you can protect them, and how you can ensure that your software distribution architecture is able to support patch management.

The key areas for ongoing assessment are:

* Inventory/discover existing computing assets.
* Assess security threats and vulnerabilities.
* Determine the best source for information about software updates.
* Software version control to maintain standard application versions.
* Assess the existing software distribution infrastructure.
* Assess operational effectiveness.

A number of tools, utilities, and products are available from Microsoft to help in the Assess phase of patch management. These include:

* [Microsoft Systems Management Server (SMS)](http://www.microsoft.com/technet/updatemanagement/plan/sms-step1.mspx)
* [Patch Management Using SMS 2003 Solution Accelerator](http://www.microsoft.com/downloads/details.aspx?FamilyId=E9EAB1BD-13E7-4E25-85C5-CE2D191C3D63&displaylang=en)
* [Microsoft Windows Server® Update Services (WSUS)](http://technet2.microsoft.com/WindowsServer/en/library/d446d310-413f-4844-8aad-c557712397401033.mspx)
* [Microsoft Baseline Security Analyzer (MBSA)](http://www.microsoft.com/technet/security/tools/mbsa2/default.mspx)
* [Microsoft Application Compatibility Toolkit (ACT)](http://technet.microsoft.com/en-us/windowsvista/aa905072.aspx)
* [Microsoft Update (MU)](http://www.microsoft.com/technet/security/smallbusiness/topics/patchmanagement/dep_patches_wu_au.mspx)
* [SMS 2003 Desired Configuration Monitoring (DCM)](http://www.microsoft.com/technet/itsolutions/cits/mo/sman/dcm.mspx)

A comparison of these tools is located at the end of this section. Microsoft partners and other third parties offer additional products and tools that can be used in the Assess phase.

## Phase 2: Identify

The goals for the Identify phase are to:

* Discover new software updates in a reliable way.
* Determine whether software updates are relevant to your production environment.
* Obtain software update source files and confirm that they are safe and will install successfully.
* Determine whether the software update should be considered an emergency.

Discovering a new software update starts with notification, which should be supplied either through a subscription to a reliable source that provides scanning and reporting activities, or by some other reliable notification mechanism. The following are the most commonly used notification mechanisms:

* E-mail notifications: <http://www.microsoft.com/technet/security/bulletin/notify.mspx>.
* Viewing updates in the Windows Server Update Service (WSUS) console toolbar.
* SMS 2003 Inventory Tool for Microsoft Updates (ITMU): <http://www.microsoft.com/technet/downloads/sms/2003/tools/msupdates.mspx>.
* Vulnerability scanning tools, such as MBSA, to scan for missing updates.

You can determine the applicability of a software update to your IT infrastructure using the following screening methods:

* Reading security bulletins and Knowledge Base articles.
* Reviewing individual software updates.

After you have obtained the update, it should be verified through the following activities:

* Identifying and verifying the software update owner.
* Reviewing all accompanying documentation.
* Ensuring that the software update is free from viruses.

## Phase 3: Evaluate and Plan

Your goal during the Evaluate and Plan phase is to make a go/no-go decision to deploy the software update, determine what resources it will take to deploy it, and test the software update in a production-like environment to confirm that it does not compromise business-critical systems and applications.

The key requirements for evaluation and planning are:

* Determine the appropriate response.
* Plan the release of the software update.
* Build the release.
* Conduct acceptance testing of the release.

To determine the appropriate response to an available update you should:

* Prioritize and categorize the request.
* Obtain authorization to deploy the software update.

Release planning is the process of working out how you will release the software update into the production environment. Following are the major considerations for planning the release of a new software update:

* Determine what needs to be patched.
* Identify the key issues and constraints.
* Build the release plan.

To build the release, you must develop the scripts, tools, and procedures that administrators will use to deploy the software update into the production environment.

Testing should be carried out, regardless of whether the software update is regarded as normal or business-critical, with the following results:

* After the software update installation is complete, the computer should restart and operate without incident.
* The software update, if it is targeted at computers connected across slow or unreliable network connections, can be downloaded across these links, and, after this completes, the software update successfully installs.
* The software update is supplied with an uninstall routine, and this can be used to successfully remove the software update.
* Business-critical systems and services continue to run after the software update has been installed, and the machine has restarted, if that is a necessary step.

A best practice is to have a testing and validation infrastructure in place to test software updates before they are put into production. Guidance for building a testing and emulation environment is provided in the [Windows Server System Reference Architecture Virtual Environments for Development and Test](http://www.microsoft.com/technet/itsolutions/wssra/ve/default.mspx).

[Microsoft Virtual Server 2005 R2](http://www.microsoft.com/downloads/details.aspx?FamilyID=6dba2278-b022-4f56-af96-7b95975db13b&DisplayLang=en) and [Microsoft Virtual PC 2004 SP1](http://www.microsoft.com/downloads/details.aspx?FamilyID=6d58729d-dfa8-40bf-afaf-20bcb7f01cd1&DisplayLang=en) are free product downloads and can be used as part of your testing and validation infrastructure.

## Phase 4: Deploy

Your goal during the Deploy phase is to successfully roll out the approved software update into your production environment so that you meet all of the requirements of any deployment service level agreements (SLAs) you have in place.

The deployment of a software update should consist of the following activities:

* Deployment preparation.
* Deployment of the software update to client computers.
* Post-deployment review.

The production environment needs to be prepared for each new release. The steps required for preparing the software update for deployment should include the following:

* Communicating the rollout schedule to the organization.
* Staging updates on distribution points.

The steps required to deploy a software update in production should include the following:

* Advertising the software update to client computers.
* Monitoring and reporting on the progress of deployment.
* Handling failed deployments.

The post-implementation review should typically be conducted within one to four weeks of a release deployment to identify improvements that should be made to the patch management process. A typical agenda for a review includes:

* Ensure that the vulnerabilities are added to your vulnerability-scanning reports and security policy standards so the attack does not have an opportunity to recur.
* Ensure that your build images have been updated to include the latest software updates following the deployment.
* Discuss expected results compared to actual results.
* Discuss the risks associated with the release.
* Review your organization’s performance throughout the incident. Take this opportunity to improve your response plan and include lessons learned.
* Discuss changes to your service windows.

## Operations

The patch management process is an ongoing and iterative cycle. While Operations is not a patch management phase in the Infrastructure Optimization Model, it is necessary that IT operations define the frequency of patching that best suits your organization’s needs and security goals. Your organization should define a system for determining the critical nature of released patches and have a service level defined for each patch release level.

## Available Tools

A number of tools and products can automate the delivery and installation of software updates. As defined in best practice patching, exercising manual control over which patches are installed to managed computers is a requirement. Allowing Automatic Updates or Microsoft Update to run unchecked does not comply with best practice patch management for organizations; however, in some cases, when dedicated IT staff is limited or users are remote and unmanaged, these technologies can be used.

The recommended options for managing software updates are Systems Management Server 2003 (SMS 2003) and Windows Server Update Services (WSUS). In addition to these options, numerous Microsoft partners and other third parties offer options to assist with patch management.

The following table lists software tools available from Microsoft to perform installation of software updates.

|  |  |  |  |
| --- | --- | --- | --- |
| **Feature** | [Microsoft Update (MU)](http://update.microsoft.com/) | [Windows Server Update Services (WSUS)](http://technet2.microsoft.com/windowsserver/en/technologies/featured/wsus/default.mspx) | [Systems Management Server 2003 (SMS 2003)](http://www.microsoft.com/smserver) |
| Content Types Supported | All software updates, driver updates, service packs (SPs), and feature packs (FPs) | Same as MU, with only critical driver updates | All updates, SPs, & FPs, supports update & app installs for any Windows-based software |
| Applicability | Individual users | Small- to mid-size businesses | Enterprise customers |

### Tool Coverage in Patch Process

The following table lists the primary tool-related functions in the patch process:

| **Product or Tool** | **Hardware & Software Inventory** | **Scans Target for Updates** | **Identifies New Updates** | **Admin Controls Installation** | **Automated Deployment** |
| --- | --- | --- | --- | --- | --- |
| [SMS 2003 with ITMU](http://www.microsoft.com/smserver) | X | X | X | X | X |
| [WSUS](http://technet2.microsoft.com/windowsserver/en/technologies/featured/wsus/default.mspx) |  | X | X | X | X |
| [MBSA](http://www.microsoft.com/technet/security/tools/mbsahome.mspx) |  | X |  |  |  |
| [ACT](http://technet.microsoft.com/en-us/windowsvista/aa905072.aspx) | X |  |  |  |  |
| [SMS 2003 DCM](http://www.microsoft.com/technet/itsolutions/cits/mo/sman/dcm.mspx) | X | X |  |  |  |

The [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905072.aspx) has been included in this table because it contains functionality to determine hardware specifications and application inventory of client computers. It also includes analysis and reporting for update impacts on applications.

Ensuring that all intended software updates and service packs are installed is a key step in managing a standard configuration. [Systems Management Server 2003 Desired Configuration Monitoring (DCM)](http://www.microsoft.com/technet/itsolutions/cits/mo/sman/dcm.mspx) has been included in this list because it will monitor compliance of a known configuration state and inform administrators if requested updates or service packs are not present on managed computers.

Patch management guidance in a future Infrastructure Optimization Implementer Resource Guide series will introduce tools and procedures for update management for servers and mobile devices.

## Further Information

For more information on patch management, visit [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search on ”Patch Management" or visit the [TechNet Update Management Solution Center](http://www.microsoft.com/technet/updatemanagement/default.mspx).

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

# *Checkpoint: Automated Patch* *Distribution to Desktops and Laptops*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | 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 Standardized level for Automated Patch Distribution in this capability based on the Infrastructure Optimization model. We recommend that you follow the guidance of additional best practice resources for configuration monitoring and management to ensure that client patch levels are maintained to a known standard.

Go to the [next Self-Assessment question](#_Do_you_have_1).

# Requirement: Defined Standard Images for Desktops and Laptops

## Audience

You should read this section if you do not have a defined set of basic images for 80 percent or more of your desktops.

## Overview

To succeed in deploying an operating system, organizations must use the best technology and business processes available, in addition to best practices for optimizing those technologies. By developing baselines for the computing environment, organizations have a known and fixed configuration for deployment, which lowers the cost of support, troubleshooting, and other operations. Through imaging, a standard build that includes core applications, the operating system, and any additional organization requirements can be used for workstation deployment. This document lists tools that are available and the steps you should take to automate and establish standard desktop images. Deployment of standard images will be covered in future documents.

## Phase 1: Assess

Most IT implementers share a common goal: to create a corporate-standard desktop configuration that is based on a common image for each operating system version in the organization. IT implementers want to apply a common image to any computer in any region at any time, and then customize that image quickly to provide services to users.

In reality, most organizations build and maintain many images—sometimes up to 100 different images. By making technical and support compromises, making disciplined hardware purchases, and using advanced scripting techniques, some organizations have reduced the number of images they maintain to a just few. These organizations tend to have the sophisticated software-distribution infrastructures necessary to deploy applications—often before first use—and keep them updated.

In the Assess Phase it is important to inventory your workstations and determine the number of active operating systems and applications in your environment. We recommend that you use a tool to automate the inventory process, such as [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx), the [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905078.aspx#ACT), or the [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=96674).

## Phase 2: Identify

During this phase you should list any current disk-imaging technologies and standard images used by your organization and identify the imaging direction, tools, and techniques you would like to implement. Advances in desktop imaging technology should prompt consideration for updating legacy imaging tools and practices.

A number of tools are available to capture a desktop image. Imaging technology can be sector-based and usually is destructive when applied to the targeted computer, or it can be file-based and nondestructive. Using file-based image technology, you can install new images in a separate partition of deployment-targeted PCs, which allows advanced in-place migration scenarios.

Microsoft offers a free command-line tool to enable disk imaging. The imaging utility, called [ImageX](http://technet.microsoft.com/en-us/windowsvista/aa905070.aspx), uses the Microsoft Windows Imaging Format (WIM) image format. Instead of a sector-based image format, the WIM image format is file-based and nondestructive. The [SMS 2003 Operating System Deployment Feature Pack](http://www.microsoft.com/technet/downloads/sms/2003/featurepacks/osdfp.mspx) also leverages ImageX technology and the WIM file format to create and deploy desktop images.

Additional tools are available in [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx) for integrating several of the steps needed to define and deploy desktop images. The Deployment Workbench, a tool contained in BDD 2007, creates distribution shares and develops disk images. Automated deployment themes in the future Implementer Resource Guides will further discuss BDD 2007 and Deployment Workbench.

## Phase 3: Evaluate and Plan

During the Evaluate and Plan Phase you discuss possible approaches your organization can use to implement a standardized desktop imaging strategy. You should weigh the costs and benefits of each imaging technology and image type to develop a strategy that best suits your organization’s needs. Factors that affect the costs associated with building, maintaining, and deploying disk images are development costs, test costs, storage costs, and network costs.

As the size of image files increases, costs increase. Large images have more updating, testing, distribution, network, and storage costs associated with them. When you update even a small portion of the image, image administrators must distribute the entire file to client computers.

The three primary strategies for standard images are:

* Thick images
* Thin images
* Hybrid images

### Thick Images

Thick images contain the operating system, applications, and other corporate-standard files. The advantage of thick images is simplicity; deployment is a single step because all files are deployed at once. Also, applications are available on first run. The disadvantages are maintenance, storage, and network costs. Thick images also limit flexibility. Either all computers receive all applications whether needed or not, or many different thick images must be developed and maintained. Using thick images is a common legacy approach.

### Thin Images

Thin images contain few if any applications. The advantages of thin images are many. They cost less to build, maintain, and test. Network and storage costs are lower. There is far greater flexibility. However, flexibility increases deployment and networking costs.

### Hybrid Images

Hybrid images are a combination of thick and thin images. In a hybrid image, the disk image is configured to install applications on first run, giving the illusion of a thick image but installing the applications from a network source. Hybrid images have most of the advantages of thin images, yet are not as complex to develop and do not require a software distribution infrastructure. Installation times are longer, which can increase initial deployment costs.

An alternative is to start with a tested thin image and build a thick image on top of it. Testing the thick image is minimized, because the imaging process is essentially the same as a regular deployment.

Another alternative is to add a minimum number of core applications to a thin image. These applications could include antivirus software and line-of-business (LOB) applications required on all computers in the company.

## Development

Recommended guidance for developing desktop images can be found in the [Solution Accelerator for Business Desktop Deployment (BDD) 2007](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx) and the [Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx). BDD 2007 discusses imaging technologies available from Microsoft and how they are used to customize, build, capture, and deploy disk images for the Windows XP SP2 and Windows Vista™ desktop operating systems.

### Test Plan

Another important part of the development stage is the creation of a test plan. You need to determine all configuration scenarios in which the disk image must work. These configurations include both hardware and business processes that client machines support. A bug reporting and tracking mechanism is important to ensure that all problems that arise in testing are addressed.

### Stabilization

The image and deployment process created in the Development stage must be fully tested and stabilized before deployment to the enterprise. You must diligently follow the test plan created in the Planning stage. All problems encountered should be logged and tracked with a bug reporting system. When all bugs are resolved, the final image or images can be deployed to client computers.

## Phase 4: Deploy

The Deploy Phase for imaging is also discussed in the [Deployment Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/deftgs_3.mspx) found in BDD 2007. The Standardized level of Infrastructure Optimization recommends leveraging Lite Touch Installation (LTI) of standard disk images.

BDD 2007 Lite Touch Installation requires minimal infrastructure. You can deploy target operating systems over the network by using a shared folder or locally by using removable storage, such as a CD, DVD, USB hard drive, or other device. The configuration settings for each individual computer are usually provided manually during the deployment process. See the BDD 2007 [Deployment Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/deftgs_3.mspx) for more details.

## Operations

Maintenance of the final image or images is an ongoing process. Updates to the operating system, device drivers, and applications must be analyzed for their applicability to your enterprise. Either they must be integrated into the existing image, or completely new images must be built. Then you must test and validate the final images before they can be deployed to client computers.

## Available Tools

Microsoft Technologies

| **Product, Tool, or Utility** | **Use** |
| --- | --- |
| [Business Desktop Deployment 2007 (BDD 2007)](http://www.microsoft.com/technet/desktopdeployment/bddoverview.mspx) | Overall image creation, capture, and deployment methodologies and tools. Uses the Deployment Workbench to integrate many of the tools and utilities listed in this table. |
| [Microsoft Windows Automated Installation Kit (AIK)](http://www.microsoft.com/downloads/details.aspx?FamilyID=c7d4bc6d-15f3-4284-9123-679830d629f2&DisplayLang=en) | The Windows AIK is a set of deployment tools supporting the latest release of Windows; it includes methods, tools, and requirements for deploying Windows. |
| [Windows Preinstallation Environment (Windows PE)](http://technet.microsoft.com/en-us/windowsvista/aa905120.aspx) | Part of Windows AIK. Windows PE is a bootable tool from Microsoft that provides operating system features for installation, troubleshooting, and recovery. |
| Windows System Image Manager (Windows SIM) | Part of Windows AIK. Windows SIM enables creation of answer files (Unattend.xml) and network shares or modification of the files contained in a configuration set. |
| [System Preparation Tool (Sysprep)](http://www.microsoft.com/technet/desktopdeployment/imaging/imagingsysprep.mspx) | Part of Windows AIK. Sysprep facilitates image creation and prepares an image for deployment to multiple client computers. |
| [ImageX](http://technet.microsoft.com/en-us/windowsvista/aa905070.aspx) | Part of Windows AIK. A command-line tool that captures, modifies, and applies installation images for deployment. |
| Windows image | A single compressed file containing a collection of files and folders that duplicate a Windows installation on a disk volume. A Windows image is created as a WIM file and can be created using ImageX or the [Systems Management Server 2003 Operating System Deployment Feature Pack](http://www.microsoft.com/technet/downloads/sms/2003/featurepacks/osdfp.mspx). |

Other Available Products

|  |  |
| --- | --- |
| **Product** | **Vendor** |
| Ghost | [Symantec](http://www.symantec.com) |
| PowerQuest | [Symantec](http://www.symantec.com) |

# *Checkpoint: Defined Standard Images for Desktops and Laptops*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Used tools to capture a standard image. |
|  | Defined a strategy for standard images. |
|  | Defined a standard set of disk images (OS and applications) for all hardware types. |
|  | Established deployment tools for network-based or offline image installation. |

If you have completed the step listed above, your organization has met the minimum requirement of the Standardized level for Defined Standard Images for Desktops and Laptops in the Desktop, Device and Server Management capabilities of the Infrastructure Optimization Model. We recommend that you follow additional best practices for image management 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](#_Do_you_have_2).

# Requirement: Centralized Management of Mobile Devices

## Audience

You should read this section if you do not have a centralized solution to track, manage, and upgrade your mobile devices.

## Overview

Organizations worldwide are using mobile devices to accelerate business cycles, increase productivity, reduce operating costs, and extend their infrastructure. With this growing reliance on mobile devices, it is critical for administrators to understand their mobile environment, to ensure users set up secure corporate access, and to deliver new business capabilities while utilizing existing infrastructure investments.

Mobile-device management is a relatively new concept and there are limited offerings from Microsoft and its partners to supplement management tools for client and server devices.

## Phase 1: Assess

In 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. To move from the Basic level to the Standardized level you need to centrally manage the following:

* Discovery and tracking of mobile hardware.
* Tracking, distribution, and updating of mobile software.
* Data synchronization.
* Proactive and reactive data security.
* Defined procedures for decommissioning retired mobile devices.

This section provides information on the tools and processes that address these areas. The following sections discuss tools from Microsoft for managing mobile devices.

## Phase 2: Identify

In the Identify Phase, your organization needs to develop and implement a solution for discovering the mobile devices connected to your network on an ongoing basis and determine the direction needed to manage mobile devices at a level consistent with your needs. 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. Identification of connected devices can be performed either manually with the user volunteering information, or by using tools to discover network-connecting devices.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan Phase, your organization should consider which tools or technologies can be used to aid mobile device management. The primary products currently available from Microsoft are Microsoft® Exchange Server with ActiveSync®, Direct Push, Remote Wipe, and Systems Management Server (SMS) 2003 with the Device Management Feature Pack. Additional products are offered from Microsoft partners and software vendors such as [Odyssey Software](http://www.odysseysoftware.com/), [Bluefire](http://www.bluefiresecurity.com/), and [iAnywhere](http://www.ianywhere.com/) to manage mobile devices.

### Exchange Server 2003 and Exchange Server 2007

Beginning with Exchange Server 2003 and continuing with Exchange Server 2007, Microsoft has introduced new capabilities for the management of Windows mobile devices. Mobile-device technologies in Exchange Server 2003 and Exchange Server 2007 are ActiveSync, Remotely Enforced Device Security Policies, and Remote Device Wipe.

Wirelessly synchronizing Microsoft® Windows Mobile®-based devices using built-in Exchange ActiveSync requires at least one server running Exchange Server in your messaging infrastructure. Note that neither Exchange 2003 nor Exchange 2007 need to be fully deployed across your organization’s entire environment to use this capability.

For information on setting up the required Exchange Server 2003 components, please see the Exchange Server 2003 deployment guide (particularly Chapter 8): <http://www.microsoft.com/technet/prodtechnol/exchange/2003/library/depguide.mspx>.

Also see the Exchange Server 2003 ActiveSync Architecture white paper: <http://www.microsoft.com/exchange/techinfo/administration/mobiledevices.asp>.

Note that earlier versions of Exchange Server do not offer built-in synchronization capabilities. You must use Exchange Server 2003 or Exchange Server 2007 for users to wirelessly synchronize their Windows Mobile-based devices.

#### Active Directory

For ActiveSync to work, your infrastructure must include Active Directory domain controllers. You also need to make sure that your Exchange Server 2003 servers are members of a Windows Active Directory domain.

Active Directory domain controllers must run on either Windows 2000 Server SP3 or Windows Server 2003. We recommend Windows Server 2003 for best performance.

#### Managing Exchange ActiveSync

By default, after you install the Client Access server role on the Exchange 2007 server, Exchange ActiveSync is enabled. End users need only configure their mobile devices to synchronize with the Exchange Server computer to use Exchange ActiveSync. Administrators can perform a variety of management tasks using Exchange ActiveSync. These include configuring Exchange ActiveSync mailbox policies and configuring authentication for increased security. You can perform some of these tasks in the Exchange Management Console and all of them in the Exchange Management Shell.

#### Managing Exchange ActiveSync Users

By default, if the Client Access server role is installed in a Microsoft Exchange organization that is running Exchange Server 2007, Exchange ActiveSync is enabled for all users. You can disable Exchange ActiveSync for a user or group of users and also manage various settings for your Exchange ActiveSync users.

To simplify management of your Exchange ActiveSync users, you can create Exchange ActiveSync mailbox policies. These policies help you apply specific settings to a single user or group of users. Available settings include the following:

* Require a password.
* Require an alphanumeric password.
* Allow attachments to be downloaded to the device.
* Allow access to Microsoft Windows SharePoint® Services documents.
* Enable device encryption.

For more information about Exchange ActiveSync mailbox policies, visit [Managing Exchange ActiveSync with Policies](http://technet.microsoft.com/en-us/library/9317b3bc-44a1-4e54-bc51-4f0b194b6a55.aspx).

For more information about how to use the Exchange Management Console to manage an Exchange ActiveSync user, see the following topics:

* [How to Enable or Disable Exchange ActiveSync for a Mailbox User](http://technet.microsoft.com/en-us/library/bb124809.aspx)
* [How to Add Users to an Exchange ActiveSync Mailbox Policy](http://technet.microsoft.com/en-us/library/aa997929.aspx)
* [How to Configure Synchronization Options for Users](http://www.microsoft.com/technet/prodtechnol/exchange/2003/autd.mspx)

#### Remotely Enforced Device Security Policies

Exchange Server 2003 SP2 and Exchange Server 2007 help you configure and manage a central policy that requires all mobile device users to protect their device with a password to access the Exchange server. Not only that, you can also specify the length of the password, require use of a character or symbol, and designate how long the device has to be inactive before prompting the user for the password again.

An additional setting, "wipe device after failed attempts," allows you to delete all data on the device after the user repeatedly enters the wrong password a specified number of times. The user will see alert dialog boxes warning of the possible wipe and providing the number of attempts left before it occurs.

Another setting allows you to specify whether noncompliant devices can synchronize. Devices are considered noncompliant if they do not support the security policy you have specified. In most cases, these are devices not configured with the Exchange Server Messaging and Security Feature Pack.

#### Remote Device Wipe

The remote wipe feature helps you manage the process of remotely erasing lost, stolen, or otherwise compromised mobile devices. If the device was connected using Direct Push technology, the wipe process will be initiated immediately and should take place in seconds. If you have used the enforced lock security policy, the device is protected by a password and local wipe, so the device will not be able to perform any operation other than to receive the remote wipe notification and report that it has been wiped.

Device security policies are managed from Exchange System Manager Mobile Services Properties window. Here you can:

* View a list of all devices that are being used by any user.
* Select or deselect devices to be remotely erased.
* View the status of pending remote-erase requests for each device.
* View a transaction log that indicates which administrators have issued remote-erase commands, in addition to the devices to which those commands pertained.

#### Certificate-Based Authentication

If Secure Sockets Layer (SSL) basic authentication does not meet your security requirements and you have an existing Public Key Infrastructure (PKI) using Microsoft Certificate Server, you may want to use the certificate-based authentication feature in Exchange ActiveSync. If you use this feature in conjunction with other features described in this document, such as local device wipe and the enforced use of a power-on password, you can transform the mobile device itself into a smart card. The private key and certificate for client authentication is stored in memory on the device. However, if an unauthorized user attempts to brute-force attack the power-on password for the device, all user data is purged, including the certificate and private key.

Microsoft has created a tool for deploying Exchange ActiveSync certificate-based authentication. To download the tool and documentation from the Microsoft Download Center, go to <http://go.microsoft.com/fwlink/?LinkId=63271>.

#### S/MIME-Encrypted Messaging

The Messaging and Security Feature Pack for Windows Mobile 5.0 provides native support for digitally signed, encrypted messaging. When encryption with the Secure/Multipurpose Internet Mail Extension (S/MIME) is deployed, end users can view and send S/MIME-encrypted messages from their mobile device.

The S/MIME control:

* Is a standard for security enhanced e-mail messages that use a PKI to share keys.
* Offers sender authentication by using digital signatures.
* Can be encrypted to protect privacy.
* Works well with any standard-compliant e-mail client.

For guidance on how to implement the S/MIME control with Exchange Server 2003 SP2, see the Exchange Server Message Security Guide at <http://go.microsoft.com/fwlink/?LinkId=63272>.

### SMS 2003 Device Management Feature Pack

The [Systems Management Server 2003 Device Management Feature Pack (DMFP)](http://www.microsoft.com/technet/downloads/sms/2003/featurepacks/dmfp.mspx) gives SMS 2003 the power to manage mobile devices running Microsoft Windows® CE (3.0 or later) and Windows Mobile software for Microsoft Pocket PCs (2002 or later), and Windows Mobile 5.0 and Windows Mobile Pocket PC Phone Edition 5.0. Using the DMFP, IT administrators can capture the asset characteristics, configuration settings, and security policies of mobile devices, and to update or deploy new applications with minimal interruption to the end user, dramatically reducing the cost of deploying and managing devices.

Using the DMFP, you can do the following:

* Discover and collect inventory information from mobile and on-site clients running Windows CE 4.2 or Windows Mobile 2003 software for Pocket PC and Pocket PC Phone Edition, and Windows Mobile 5.0 and Windows Mobile Pocket PC Phone Edition 5.0.
* Through complementary partner offerings, discover and collect inventory from mobile and on-site clients running Windows CE 3.0, Pocket PC 2002 software, Windows Mobile 5.0 and Windows Mobile Pocket PC Phone Edition 5.0, and Windows Mobile software, including smart phones.
* Distribute software updates and applications to these devices.
* Support regional roaming scenarios for SMS package downloads by referring clients to local distribution points.
* Implement password policy by enforcing secure passwords for these devices.
* Deploy the SMS client software to devices with an ActiveSync connection to a computer running the SMS Advanced Client.
* Use HTTP or secure HTTP (HTTPS) to communicate with the SMS server infrastructure.

Using these technologies, you can control mobile devices using Microsoft operating systems and software. Exchange Server’s device management capabilities are the minimum required set of capabilities to achieve the Standardized level in the Infrastructure Optimization Model.

## Phase 4: Deploy

The goal of the Deploy Phase is to implement the selected technologies or features required to support your device management strategy. Because corporate network configurations and security policies vary, the deployment process will vary for each mobile messaging system installation. This deployment process includes the required steps and the recommended steps for deploying a mobile messaging solution that uses Exchange Server 2003 SP2 and Windows Mobile 5.0–based devices.

For detailed guidance to deploy a secure mobile messaging using Microsoft Exchange Server, see the [Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2](http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx).

## Operations

The goal of ongoing Operations is to ensure a secure and highly available mobile messaging environment for end users. Visit the [Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx) at Microsoft TechNet for guidance on [maintaining your mobile messaging environment](http://www.microsoft.com/technet/solutionaccelerators/mobile/maintain/default.mspx).

## Further Information

For more information on managing mobile devices, visit [Microsoft TechNet](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx) and search on “mobile device management.”

To see how Microsoft handles one aspect of mobile device management, go to <http://www.microsoft.com/technet/itshowcase/content/mobmess_tcs.mspx>.

# *Checkpoint: Centralized Management of Mobile Devices*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed software to discover and track the mobile devices in your organization. |
|  | Implemented password-controlled access. |
|  | Established centralized data and software synchronization. |
|  | Ensured that decommissioned devices are free of company information. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Centralized Tracking, Management, and Upgrading of Mobile Devices. We recommend that you follow additional best practices for mobile device management addressed in the [Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx) at Microsoft TechNet.

Go to the [next Self-Assessment question](#_Do_you_have_3).

# Requirement: Identity Validation, Data Protection, and Data Backup of Mobile Devices

## Audience

You should read this section if you do not have user identity validation and data protection and backup for mobile devices.

## Overview

Lost or stolen mobile devices can compromise sensitive corporate information and allow access to corporate networks. You must protect these resources by implementing thorough policies and software. In this section of the guide we address areas where you can take steps to secure corporate information and networks in your organization. These areas are:

* User access
* Passwords
* Device lockout
* Certificates
* Data access
* Data encryption
* Remote device wipe

For information about mobile device security from Microsoft, go to <http://www.microsoft.com/windowsmobile/business/5/default.mspx>.

## Phase 1: Assess

The primary goals in the Assess Phase are to determine how users are accessing data and to collect the business needs for ensuring secure access and data protection for mobile devices. Most of these principles were addressed during the Plan and Deploy Phases of the Centralized Management of Mobile Devices section of the guide. This capability in the Infrastructure Optimization Model reinforces the importance of data security and controlled user access.

## Phase 2: Identify

During the Identify Phase you will identify technology options and develop requirements to meet your organization’s requirements for user access, data security, and data backup. Refer to the [Requirement: Centralized Management of Mobile Devices](#_Centralized_Tracking,_Management,) section of this guide for detailed information about the technologies and features available in Microsoft Exchange Server 2003, Microsoft Exchange Server 2007, and Systems Management Server 2003

Also, visit the [Windows Mobile Center](http://www.microsoft.com/technet/itsolutions/mobile/default.mspx) at Microsoft [TechNet](http://www.microsoft.com/technet) for more details.

## Phase 3: Evaluate and Plan

The goal of the Evaluate and Plan Phase is to develop a detailed strategy for secure user access, data security, and data protection of managed mobile devices. High-level considerations of these objectives are described in this section.

### User Access

The first defense against unauthorized access to information on a mobile device is user identification and validation using passwords or certificates.

#### Passwords

Access to each of your organization’s mobile devices should require a password. Passwords can be either simple (numeric) or strong (comprised of letters, numbers, and special characters), as dictated by your company password policy.

#### Device Lockout

If a user repeatedly fails to enter the correct password a predetermined number of times (usually three to five) the mobile device should enter a lockout state where further access can only be accomplished by an administrative reset.

#### Certificates

A public key certificate, usually called simply *a certificate*, is a digitally signed statement that is commonly used for authentication and to secure information on open networks. A certificate securely binds a public key to the entity that holds the corresponding private key. The issuing certification authority (CA) digitally signs the certificates, and they can be issued for a user, a computer, or a service. You must have procedures in place to revoke certificates when a mobile device is lost or stolen.

### Data Access

Whenever a mobile computer is outside the organization's physical security boundary, theft of the computing device and the data it contains is a primary concern. If theft does occur, the initial problem of lost data escalates to potentially having an unauthorized person penetrate the network via remote dial-up or wireless networking. Because of their design, mobile computers and many new types of portable devices have a higher risk of being stolen than a nonportable device. Often these machines hold important company data and represent a security risk if stolen.

#### Data Encryption

You can use an encrypted file system on mobile devices to obscure data on the hard drive, which renders it useless to anyone without proper credentials. This protects the data from access by someone that obtains a device that has been lost or stolen.

#### Remote Device Wipe

Features of Exchange Server remote device wipe allow an administrator or an authorized user the ability to remotely erase all information on a mobile device, effectively returning it to its initial default state.

As a reactive measure, you can use remote wipe to block unauthorized access to the data on a lost or stolen mobile device. You would use remote wipe if you conclude that other access provisions such as passwords or certificates were not in place, or had been compromised. In this scenario, a command to wipe the device is sent from a server.

Proactively, remote wipe can be another tool you can use along with user authentication and data encryption to ensure that access to corporate data and the company network can be blocked if the mobile device has been stolen. In this scenario the device self-wipes based on the imbedded security policy.

### Data Backup

Data backup of sensitive messaging, calendar, and company address list data is a critical first step for data backup on mobile devices. Data backup for synchronized messaging, address list, and calendar information is performed by the Exchange Server infrastructure via standard server backup and recovery procedures. See the Standardized level Infrastructure Optimization [Backup and Restore Services for Critical Servers](#_Defined_Backup_and_1) section of this guide for more details. Additionally, software is available from Microsoft partners to perform device-level backups of nonsynchronized data.

## Phase 4: Deploy

The goal of the Deploy Phase is to implement your organization’s selected strategy for managing user access, data security, and data backup. For detailed guidance on deploying the technologies outlined in this guide, go to the [Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2](http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfpdepguide.mspx).

## Operations

The goal of ongoing Operations is to ensure secure user access, data security, and data backup in your mobile messaging environment. Visit the [Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx) at Microsoft TechNet for guidance on [maintaining your mobile messaging environment](http://www.microsoft.com/technet/solutionaccelerators/mobile/maintain/default.mspx).

## Further information

For more information on remote wipe, go to  
<http://www.microsoft.com/technet/prodtechnol/exchange/e2k7help/7b2cb90a-67f5-45d5-8c7a-26309faa7d9e.mspx?mfr=true>.

# *Checkpoint: Identity Validation, Data Protection, and Data Backup of Mobile Devices Checkpoint*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Established and are enforcing a password-access policy or using public key certificates for user identification. |
|  | Encrypted all transfers for data distribution to, and data backup from, mobile devices. |
|  | Implemented device lockout on mobile devices. |
|  | Ensured that company information can be removed with remote wipe in case a mobile device is lost or stolen. |

If you have completed the steps listed above, your organization has met the minimum requirements of the Standardized level for Identity Validation, Data Protection, and Data Backup of Mobile Devices. We recommend that you follow additional best practices for mobile-device management addressed in the [Windows Mobile Center](http://www.microsoft.com/technet/itsolutions/mobile/default.mspx) at Microsoft [TechNet](http://www.microsoft.com/technet).

Go to the [next Self-Assessment question](#_Do_you_have_4).

# Requirement: Consolidation of Desktop Images to Two Operating System Versions

## Audience

You should read this section if you are managing more than two operating system versions in your desktop environment.

## Overview

There are several things to consider when deploying multiple operating systems within an enterprise. These include:

* Maintenance of multiple standard images.
* Availability of patches and updates.
* Cost of extended maintenance contracts.
* User productivity.
* Application compatibility.

This guide highlights the high-level considerations for consolidating your desktop images to two operating systems.

## Phase 1: Assess

The goal of the Assess Phase in image consolidation is to determine the current number of operating systems managed by your organization. We recommend that you use a tool to automate the inventory process, such as [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx), the [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905078.aspx#ACT) or the [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=96674).

## Phase 2: Identify

In the Identify Phase you begin to determine the dependencies of the operating systems discovered with your inventory and how they relate to applications used and hardware specifications.

## Phase 3: Evaluate and Plan

The purpose of the Evaluate and Plan Phase is to discuss options in consolidating your desktop images to two standard images. These include the management benefit, business benefit, and prioritization of user upgrades. This section introduces many considerations of evaluating the consolidation of desktop images.

#### Multiple Standard Images

The topic "Defined Standard Images for Desktops and Laptops" earlier in this document describes the advantages of establishing and maintaining a standard desktop operating system image, and the pros and cons of thick, thin, and hybrid images. The creation and maintenance of multiple thick and hybrid images, and accompanying cost, increases associated with each different operating system that your organization must support. To move from the Basic level in the Infrastructure Optimization Model to the Standardized level you should limit the number of operating systems that you must support in your organization to a maximum of two, although limiting to only one version offers substantial benefits and is preferable.

#### Patches and Updates

Patches and updates to operating systems and applications must be tested before they are distributed to users. The time and expense involved in testing an application increases with each operating system on which the application runs. Simply tracking all available patches and updates can become time-consuming and costly.

#### Maintenance Contracts

If your organization purchases maintenance contracts for operating systems and applications, the costs can increase as the number of supported software titles increases. This is especially true of legacy operating systems and applications, software that has been retired by the vendor.

#### User Productivity

When users move from one operating system to a different one, there is a learning period that impacts productivity. The user has to stop and think about how to perform a task that was reflexive on the previous operating system.

#### Application Compatibility

As applications and operating systems are upgraded, data files on which those applications operate are not always compatible with newer versions. Standardizing on one or two operating systems and their compatible applications will minimize the problems of incompatible data files.

#### Exceptions

It is not always possible to make one or two operating systems work for every situation or organizational need. The use of mobile devices is increasing; their operating systems will differ from a desktop or laptop computer. Some end users, such as graphic designers or engineers, remote users, or vendors connecting to your network may have different operating systems on their computers than the organization standard. It is the IT department’s responsibility to account for these exceptions and to adapt the recommendations of this guide to these situations.

Other exceptions may be outside the responsibility of the IT department. Software-development organizations need to ensure that the software they are developing will run on multiple operating systems. A test lab that evaluates new operating systems and upgrades falls outside the scope of this document.

## Phase 4: Deploy

After you have determined the strategy for image consolidation, during the Deploy Phase you take into account how images are built, deployed, and maintained. See the [Computer Imaging System Feature Team Guide](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/ComImgFea_3.mspx) found in BDD 2007, or see the [Requirement: Defined Standard Images for Desktops and Laptops](#_Requirement:_Defined_Standard) resource guidance.

## Operations

After a successful operating system consolidation project has been completed, it should be understood that the release of new desktop operating system products and technologies will require careful consideration. Preparing for the new operating system will mean in most cases that the older of the two active operating systems will be phased out as the new operating system image is introduced. This ensures that the benefit of maintaining two operating system images remains intact.

# *Checkpoint: Consolidation of Desktop Images to Two Operating System Versions*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented an image-consolidation strategy. |
|  | Reduced the number of production operating systems to no more than two. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Consolidation of Desktop Images to Two Operating System Versions in the Desktop, Device and Server Management capabilities of the Infrastructure Optimization Model. We recommend that you follow additional best practices for image consolidation and management 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](#_Do_you_have_5).

Capability: Security and Networking

# Introduction

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

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Lack of basic security standards to protect against malicious software and attacks  Antivirus updates are not managed well, increasing attack risk  Help desk is reactive, spending majority of time on security-related issues  **IT Challenges**  IT workers manually perform updates and deploy patches on each machine  Irregular, unpredictable server outages mean outages in network services, reducing end-user productivity  Network administrators individually manage IP addresses to avoid duplication, and manually apply configuration changes to workstations | **Projects**  Deploy firewall with lock-down configuration (possibly a multi-tier firewall solution)  Implement networking services such as DNS server to easily find and access network services, and DHCP server for automatic, centralized IP address management  Implement a managed, standardized antivirus solution for desktops | **Business Benefits**  Established policy standards provide a more consistent computing environment  Improved desktop security by rapidly and reliably delivering patches to targeted vulnerabilities  **IT Benefits**  Centrally managed patches provide a more stable and secure infrastructure  Efficient and reliable TCP/IP network configuration helps prevent IP address conflicts and conserves the use of IP addresses through centralized management of address allocation  Controlled, robust environment that can withstand attacks through security ”layers” at the perimeter, server, desktop, and application levels  Reduced complexity of hardware and software operations lead to smoother change management processes |

The Standardized level in the Infrastructure Optimization Model addresses key areas of networking and security components, including:

* Antivirus Software for Desktops
* Centralized Firewall Services
* Internally Managed Basic Networking Services (DNS, DHCP, WINS)
* Availability Monitoring of Critical Servers

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

# Requirement: Antivirus Software for Desktops

## Audience

You should read this section if you do not have antivirus software with automated signature updating running on 80 percent of more of your desktops.

## Overview

Every organization should develop an antivirus solution that will provide a high level of protection to its network and technology resources. However, many networks still become infected, even after the installation of antivirus software. This section provides information on successfully approaching the problem of malicious software (also called malware).

## Phase 1: Assess

In the Assess Phase, your organization needs to take an inventory of managed desktop systems and determine their hardware specifications, operating systems, applications, and whether antivirus software or other malicious software-detection software is currently installed. We recommend that you use a tool to automate the inventory process, such as [Systems Management Server (SMS) 2003](http://www.microsoft.com/technet/prodtechnol/sms/sms2003/opsguide/ops_7675.mspx), the [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905078.aspx#ACT), or the [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=96674).

## Phase 2: Identify

The goal of the Identify Phase in determining an antivirus strategy is to define your organizational needs for security. Antivirus products vary by manufacturer and offer varying levels of protection and coverage against non-virus threats. Using the information gathered in the Assess Phase, your organization will be able to determine the compatibility requirements of antivirus software and identify the correct solution for your organization.

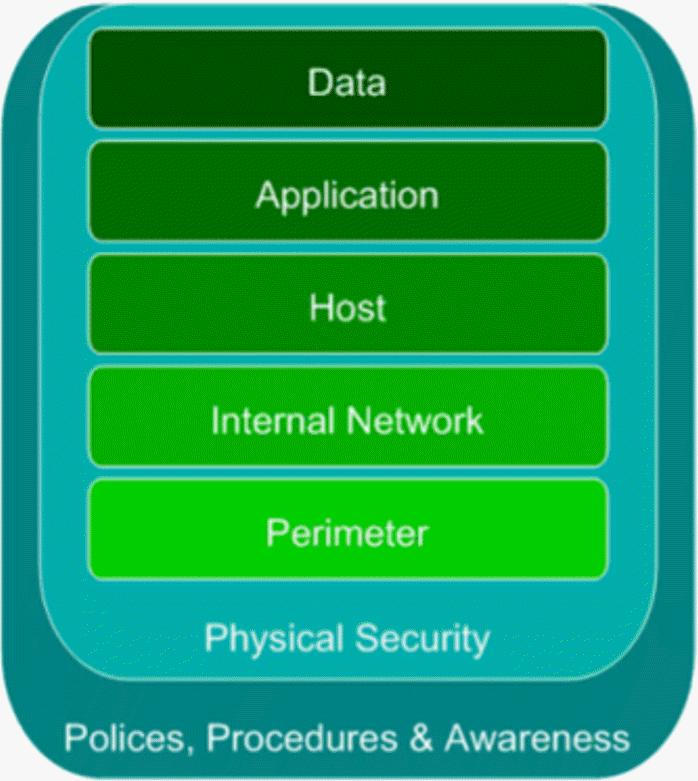
## Phase 3: Evaluate and Plan

As with network security measures, Microsoft recommends a defense-in-depth approach to antivirus design to help ensure that the safeguards your organization adopts will be properly designed and reliably maintained.

Such an approach is vital to the computer security of your organization, because unfortunately, regardless of how many useful features or services a computer system provides, someone will try to find a vulnerability to exploit for malicious purposes.

### Levels of Defense

The following figure indicates the levels within an organization that are vulnerable to a malicious software attack.



This section of the guide addresses the need for an antivirus plan for the host, application, and data levels, specifically, for client desktop computers within the organization. The other levels are covered in other documents in this series.

### Client Defenses

When malicious software reaches a host computer, defense systems must focus on protecting the host system and its data and stopping the spread of the infection. These defenses are no less important than the physical and network defenses in your organization’s network environment. You should design your host defenses based on the assumption that the malicious software has found its way through all outer layers of defense. This approach is the best way to achieve the highest level of protection.

## Phase 4: Deploy

In the Deploy Phase, you should implement a number of approaches and technologies for client antivirus protection. The following sections provide details that Microsoft recommends for consideration.

### Step 1: Reduce the Attack Surface

The first line of defense at the application layer is to reduce the attack surface of the computer. All unnecessary applications or services should be removed or disabled on the computer to minimize the number of ways an attacker could exploit the system.

### Step 2: Apply Security Updates

The sheer number and variety of client machines that may be connected to an organization's networks can make it difficult to implement a fast and reliable security update management service. Microsoft and other software companies have developed tools you can use to help manage this problem. For more detailed information on operating system patch distribution, see the section Requirement: Automated Patch Distribution to Desktops and Laptops in this guide.

### Step 3: Enable a Host-Based Firewall

The host-based or personal firewall represents an important layer of client defense that you should enable, especially on laptops that end users may take outside your organization's usual network defenses. These firewalls filter all data that is attempting to enter or leave a particular host computer.

### Step 4: Install Antivirus Software

You can choose from multiple antivirus solutions on the market, each of which attempts to protect the host computer with minimal inconvenience to and interaction with end users. Most of these applications have become very effective in providing this protection, but they all require frequent updates to keep up with new malicious software. Any antivirus solution should provide a rapid and seamless mechanism to ensure that updates to the required signature files—files that contain information antivirus programs use to detect and address malicious software during a scan, and which are regularly updated by antivirus application vendors—are delivered to the client computer as quickly as possible.

Note, however, that such updates present their own security risk, because signature files are sent from the antivirus application's support site to the host application (usually via the Internet). For example, if the transfer mechanism used to obtain the file is File Transfer Protocol (FTP), the organization's perimeter firewalls must allow this type of access to the required FTP server on the Internet. Ensure your antivirus risk assessment process reviews the update mechanism for your organization, and that this process is secure enough to meet your organization's security requirements.

### Step 5: Test with Vulnerability Scanners

After you have configured a system or network, you should check it periodically to ensure that no security weaknesses exist. To assist you with this process, a number of applications act as scanners to look for weaknesses that both malicious software and hackers may attempt to exploit. The best of these tools update their own scanning routines to defend your system against the latest weaknesses.

## Operations

As with most software, antivirus applications require a mechanism to allow continuous updates. The [Automated Patch Distribution](#_Automated_Patch_Distribution) section earlier in this guide discusses in depth the process requirements and tools available to automate software updates. Additionally, we recommend that your organization require the selected antivirus software to be running at all times. The Core Infrastructure Optimization Model Standardized to Rationalized Implementer Resource Guide will discuss how the antivirus software can be enforced to run at all times using Group Policy.

## Suggested Antivirus Software

The following software products have been tested by Microsoft to work with Microsoft operation systems:

* [Microsoft Forefront Client Security](http://www.microsoft.com/technet/clientsecurity/default.mspx)  
  by Microsoft Corporation
* [CA Anti-Virus 2007 (formerly eTrust)](http://home2.ca.com/servlet/ControllerServlet?Action=DisplayPage&Locale=en_US&id=ProductDetailsPage&SiteID=caconsum&productID=50698000&Env=BASE&ClickID=c7ekqwvep4wknnplfklkqpnkp7ekp7sweea)by CA, Inc.
* [Symantec AntiVirus Corporate Edition](http://www.symantec.com/enterprise/products/overview.jsp?pcid=1322&pvid=805_1)by Symantec Corporation
* [Norton AntiVirus 2006](http://www.symantec.com/home_homeoffice/products/sysreq.jsp?pcid=is&pvid=nav2007)  
  by Symantec Corporation
* [Rising Antivirus Software Personal Edition](http://www.ruilung.com.sg/ravp/index.asp)  
  by Beijing Rising Technology Co., Ltd.

## Further Information

For more information on implementing antivirus software, go to [The Antivirus Defense-in-Depth Guide](http://www.microsoft.com/technet/security/guidance/serversecurity/avdind_0.mspx).

To see how Microsoft approaches antivirus issues, go to <http://www.microsoft.com/technet/itshowcase/content/msghygiene.mspx>.

# *Checkpoint: Antivirus Software for Desktops*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed all operating system and software application security updates. |
|  | Enabled available host-based firewalls. |
|  | Installed antivirus software on 80 percent or more of your desktop computers. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Antivirus Software for Desktops. We recommend that you follow additional best practices for antivirus protection addressed at the [Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx).

Go to the [next Self-Assessment question](#_Do_you_have_6).

# Requirement: Centralized Firewall Services

## Audience

You should read this section if you do not have a centralized (not per desktop) firewall protecting 80 percent or more of your system.

## Overview

Firewalls are a key part of keeping networked computers safe and secure. All computers need the protection of a firewall, whether it’s the thousands of servers and desktops that compose the network of a Fortune 500 company, a traveling salesperson’s laptop connecting to the wireless network of a coffee shop, or your grandmother’s new PC with a dial-up connection to the Internet.

This section of the guide looks at both network and host-based firewalls (also called personal firewalls). Although home users have traditionally used only host-based firewalls, recent trends in security breaches highlight the importance of using both types of firewalls combined. The Standardized optimization level in the Infrastructure Optimization Model does not require host-based firewalls; these are introduced later in the model. This guide discusses all five primary classes of firewall technology.

The following guidance is based on the [Firewall Services Implementation Guides](http://www.microsoft.com/technet/itsolutions/wssra/raguide/firewallservices/default.mspx) of the [Windows Server System Reference Architecture](http://www.microsoft.com/wssra).

## Phase 1: Assess

The Assess Phase of implementing a firewall strategy addresses the business need for securing data and access to data stores and determines what, if any, firewall infrastructure is available. Every organization maintains some sensitive information that can harm the organization if it falls into the wrong hands. The potential for such harm becomes even higher, and its impact greater, if an organization actively uses the Internet for hosting various applications and services such as:

* General information-gathering and research.
* Obtaining financial market data.
* Providing online retail services.
* E-mail communications.
* Virtual private networks (VPNs) for remote workers.
* VPN-based branch office connectivity.
* Voice communications.

To provide even the most common of such services, for example e-mail, organizations must connect their internal systems to the Internet. In doing so, these systems become accessible to external sources and, therefore, vulnerable to attack. Organizations are also subject to the costs that such connections require, including payments to an Internet service provider (ISP) and investments in technologies that can protect their information systems.

Clearly, it is important to prevent information system attacks, to legally prosecute those who perpetrate them, and to be as knowledgeable as possible about the risks from different kinds of attacks.

## Phase 2: Identify

The Identify Phase explores the technology available to protect your organization’s information and provides the input necessary to evaluate your firewall options and begin planning the implementation of firewall technology.

### Types of Firewalls

There are two main types of firewalls: network firewalls and host-based (personal) firewalls. Network firewalls, such as the software-based [Microsoft® Internet Security and Acceleration Server (ISA Server)](http://www.microsoft.com/technet/isa/default.mspx), or hardware-based switched firewall systems, protect the perimeter of a network by watching traffic that enters and leaves the network. Host-based firewalls protect an individual computer regardless of the network it’s connected to. You might need one or the other—but most organizations require a combination of both to meet their security requirements.

Firewalls can be further divided into five classes:

Class 1 – Personal Firewall. These are host-based software firewalls that protect a single computer.

Class 2 – Router Firewall

Class 3 – Low-End Hardware Firewall

Class 4 – High-End Hardware Firewall

Class 5 – High-End Server Firewall

### Network Firewalls – Classes 2-5

Network firewalls protect an entire network by guarding the perimeter of that network. Network firewalls forward traffic to and from computers on an internal network, and filter that traffic based on the criteria the administrator has set.

Network firewalls can be either hardware or software based. Hardware-based network firewalls are generally cheaper than software-based network firewalls, and are the right choice for home users and many small businesses. Software-based network firewalls often have a larger feature set than hardware-based firewalls, and might fit the needs of larger organizations. Software-based firewalls can also run on the same server as other services, such as e-mail and file sharing, allowing small organizations to make better use of existing servers.

When addressing secure network connectivity, administrators need to consider the following:

* Security
* Management complexity
* Cost

By addressing these key security challenges, organizations can achieve greater employee productivity, decrease costs, and improve business integration.

### Firewall Features

Depending on the features that a firewall supports, traffic is either allowed or blocked using a variety of techniques. These techniques offer different degrees of protection based on the capabilities of the firewall. The following firewall features are listed in increasing order of complexity, and are explained in the following sections:

* Network Adapter Input Filters
* Static Packet Filters
* Network Address Translation (NAT)
* Stateful Inspection
* Circuit-Level Inspection
* Proxy
* Application-Layer Filtering

#### Network Adapter Input Filters

Network adapter input filtering examines source or destination addresses and other information in the incoming packet and either blocks the packet or allows it through. This filtering applies only to incoming traffic.

#### Static Packet Filters

Static packet filters match IP headers to determine whether or not to allow the traffic to pass through the interface. This filtering applies to both incoming and outgoing traffic.

#### Network Address Translation (NAT)

NAT converts a private address to an Internet address. Although NAT is not strictly a firewall technology, concealing the real IP address of a server prevents attackers from gaining valuable information about the server.

#### Stateful Inspection

In stateful inspection, all outgoing traffic is logged into a state table. When the connection traffic returns to the interface, the state table is checked to ensure that the traffic originated from this interface.

#### Circuit-Level Inspection

With circuit-level filtering it is possible to inspect sessions, as opposed to connections or packets.

#### Proxy

A proxy firewall gathers information on behalf of the client and returns the data it receives from the service back to the client.

#### Application-Layer Filtering

The most sophisticated level of firewall traffic inspection is application-level filtering. Good application filters allow you to analyze a data stream for a particular application and provide application-specific processing.

In general, firewalls that provide complex features will also support simpler features. However, you should read vendor information carefully when choosing a firewall because there can be subtle differences between the implied and actual capability of a firewall. Selection of a firewall typically involves inquiring about its features, and testing to ensure that the product can indeed perform according to specifications.

## Phase 3: Evaluate and Plan

Your organization’s goal during the Evaluate and Plan Phase should be to determine a strategy for firewall service. This strategy will cover three primary elements of firewall design:

**Perimeter firewall design:** A firewall solution designed to protect the enterprise infrastructure from nonsecured network traffic originating from the Internet.

**Internal firewall design:** A second firewall boundary designed to protect the traffic between semi-trusted network elements and internal trusted elements.

**Proxy design:** The proxy solution provides a mechanism to provide secure and manageable outbound communications for hosts on internal networks.

Each of these technology solutions needs to meet specific service-level goals, in addition to design goals such as availability, security, and scalability.

## Phase 4: Deploy

The goal of the Deploy Phase is to implement the strategy your organization selected and tested in the Evaluate and Plan Phase. Specific deployment routines will vary depending on the classes of firewall selected. For information on installing software-based ISA Server 2006 Enterprise Edition firewall technology, see the [ISA Server 2006 Enterprise Edition Installation Guide](http://www.microsoft.com/technet/isa/2006/installation_ee/default.mspx?mfr=true).

## Operations

Operational considerations for firewall services include managing network security, protecting the network, detecting intrusions, and reacting and implementing standardized operational requirements. To get more information about ISA Server 2006 operations tasks, such as administration, monitoring, performance, and troubleshooting to maintain your ISA Server system for optimal service delivery, visit [Microsoft ISA Server 2006 – Operations](http://www.microsoft.com/technet/isa/2006/operations/default.mspx) at Microsoft TechNet.

## Further Information

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

To see how Microsoft manages firewalls and other security risks, go to <http://www.microsoft.com/technet/itshowcase/content/securitywebapps.mspx>.

# *Checkpoint: Centralized Firewall Services*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed a centralized hardware or software firewall. |

If you have completed the step listed above, your organization has met the minimum requirement of the Standardized level for Centralized Firewall Services.

We recommend that you follow additional best practices for firewalls addressed in the [Firewall Services Implementation Guides](http://www.microsoft.com/technet/itsolutions/wssra/raguide/firewallservices/default.mspx) of the [Windows Server System Reference Architecture](http://www.microsoft.com/wssra).

Go to the [next Self-Assessment question](#_Do_you_have_7).

# Requirement: Internally Managed Basic Networking Services (DNS, DHCP, WINS)

## Audience

You should read this section if you do not have internal servers for basic networking services.

## Overview

IT networks in today's organizations have multitudes of computing devices, ranging from high-end servers to personal computers, which need to communicate with each other over the local area network (LAN). To do so, each device needs to have an identity in the form of either a logical device name (chosen by the organization) or an address that uniquely identifies the device and its location on the network.

For small networks (those with up to 500 devices), it is possible to maintain and distribute names and addresses manually, but as networks grow in size and complexity, the maintenance of an effective name resolution service becomes more and more time consuming and resource-intensive.

DNS, DHCP, and WINS are three mechanisms that are essential to the provision of IP address allocation and management services in enterprise environments. There are alternative mechanisms, but in most cases DNS and DHCP provide the backbone of any service, and WINS fulfills any requirement to collocate DNS and NetBIOS addressing schemes.

The following guidance is based on the [Windows Server System Reference Architecture Introduction to Network Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/networkservices/default.mspx).

## Phase 1: Assess

The goal of the Assess Phase for basic networking services is to define the business need for name resolution and what infrastructure, if any, is currently in place. With the widespread adoption of directory services that provide simplified access to enterprise resources, name resolution has now become a key network service. Directory services need a reliable and efficient name resolution system so that users, client operating systems, and servers can locate resources using names rather than addresses. These functions need to be performed without compromising the security of the network or the services the network provides.

## Phase 2: Identify

After your organization has assessed its need for name resolution, you should begin to identify the technologies that match your requirements.

### Domain Name System (DNS)

The primary purpose of DNS is to translate easy-to-remember, human-readable host names into numeric IP addresses. Among its many other functions, DNS also resolves e-mail addresses to locate the relevant recipient mail exchange server.

### Dynamic Host Configuration Protocol (DHCP)

DHCP is a protocol that allows a computer, router, or other network device to request and obtain a unique IP address and other parameters such as a subnet mask from a server that holds a list of available IP addresses for a network.

### Windows Internet Naming Service (WINS)

Windows Internet Naming Service (WINS) is a NetBIOS name-resolution service that allows client computers to register their NetBIOS names and IP addresses in a dynamic, distributed database and to resolve the NetBIOS names of network resources to their IP addresses.

WINS and DNS are both name-resolution services for TCP/IP networks. While WINS resolves names in the NetBIOS namespace, DNS resolves names in the DNS domain namespace. WINS primarily supports clients that run earlier versions of Windows, and applications that use NetBIOS. Microsoft Windows 2000, Microsoft Windows XP, and Windows Server 2003 use DNS names in addition to NetBIOS names. Environments that include some computers that use NetBIOS names and other computers that use domain names must include both WINS servers and DNS servers. If all computers in your networks are running Windows 2000 and later operating systems, you should use Active Directory instead of WINS.

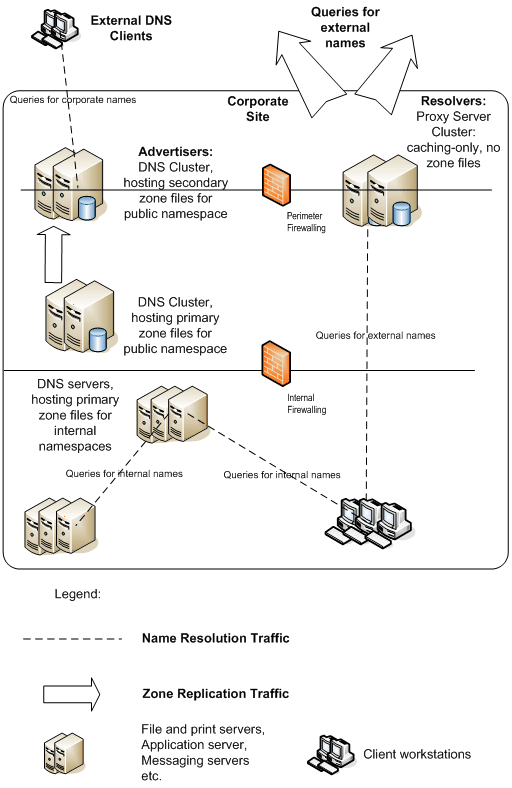
## Phase 3: Evaluate and Plan

After you have identified name resolution organizational needs and the network services required to implement, it is important to evaluate the proposed technology and how it will support your organizational goals.

### Internal DNS Server

Typically, Windows Server 2003 DNS is deployed in support of Active Directory directory service. In this environment, DNS namespaces mirror the Active Directory forests and domains used by an organization. Network hosts and services are configured with DNS names so they can be located in the network. They are also configured with DNS servers that resolve the names of Active Directory domain controllers. Windows Server 2003 DNS is also commonly deployed as a non-Active Directory, or standard, DNS solution, for hosting the Internet presence of an organization, for example.

Establishing internal DNS servers gives you the greatest flexibility and control over both internal and external domain name resolution. This reduces both intranet and Internet network traffic. The following figure illustrates how Active Directory-integrated zones and file-based secondary zones can be deployed together to provide enterprise DNS services.



### Internal DHCP Server

In Windows Server 2003, the DHCP service provides the following benefits:

Reliable IP address configuration. DHCP minimizes configuration errors caused by manual IP address configuration, such as typographical errors, or address conflicts caused by the assignment of an IP address to more than one computer at the same time.

Reduced network administration. DHCP includes the following features to reduce network administration:

* Centralized and automated TCP/IP configuration.
* The ability to assign a full range of additional TCP/IP configuration values by using DHCP options.
* The efficient handling of IP address changes for clients that must be updated frequently, such as those for portable computers that move to different locations on a wireless network.
* The forwarding of initial DHCP messages by using a DHCP relay agent, thus eliminating the need to have a DHCP server on every subnet.

### WINS and Internal Resources

Windows Server 2003 components that require name resolution will attempt to use this DNS server before attempting to use the previous default Windows name resolution service, WINS. If your organization has computers that are running operating systems earlier than Windows 2000, you will need to implement WINS for those systems. As you move from the Basic Infrastructure Optimization level to the Standardized level, you will be consolidating your IT environment by running at most only two operation systems. You will be replacing earlier systems and standardizing on newer operating systems, eliminating the need for WINS in your organization.

## Phase 4: Deploy

The goal of the Deploy Phase is to implement the technologies selected to enable basic networking services required for name resolution. For detailed guidance for deploying DNS and DHCP, see the [Deploying Network Services](http://technet2.microsoft.com/WindowsServer/en/library/119050c9-7c4d-4cbf-8f38-97c45e4d01ef1033.mspx) guidance found in the [Windows Server 2003 Deployment Guide](http://technet2.microsoft.com/WindowsServer/en/library/c283b699-6124-4c3a-87ef-865443d7ea4b1033.mspx).

## Further Information

* For more information on DNS, go to <http://technet2.microsoft.com/WindowsServer/f/?en/library/54375efb-2192-49b7-a823-57c08c6cc06c1033.mspx>.
* For further information on DHCP, go to <http://technet2.microsoft.com/WindowsServer/f/?en/library/85add012-1c2c-41bb-b1ae-11bc07485ee31033.mspx>.
* For further information on WINS, go to <http://technet2.microsoft.com/WindowsServer/f/?en/library/0bef84d9-dafe-4fa8-9e70-fb4f56f1af971033.mspx>.

# *Checkpoint: Internally Managed Basic Networking Services (DNS, DHCP, WINS)*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented DNS services on servers or other devices within your organization. |
|  | Implemented DHCP services on servers or other devices within your organization. |
|  | Implemented WINS services for older operating systems on servers or other devices within your organization. |

If you have completed the step listed above, your organization has met the minimum requirement of the Standardized level for Internally Managed Basic Networking Services (DNS, DHCP, WINS).

We recommend that you follow additional best practices for firewalls addressed in the [Network Services Implementation Guides](http://www.microsoft.com/technet/itsolutions/wssra/raguide/networkservices/default.mspx) of the [Windows Server System Reference Architecture](http://www.microsoft.com/wssra).

Go to the [next Self-Assessment question](#_Do_you_have_8).

# Requirement: Availability Monitoring of Critical Servers

## Audience

You should read this section if you do not monitor 80 percent or more of your critical servers.

## Overview

The efficiency and productivity of your organization’s computing infrastructure depends on the continuous availability of critical servers such as DNS, DHCP, File and Print, and e-mail servers. You need to establish policies and procedures to monitor these servers to quickly become aware of decreased performance or interruptions of service. Software is available to automate this monitoring and send alerts to the appropriate people so that they can take corrective steps.

## Phase 1: Assess

In the Assess Phase of Availability Monitoring of Critical Servers 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.

## Phase 2: Identify

After all servers have been inventoried, the Identify Phase is primarily a prioritization of servers and classification of which servers are critical enough to require availability monitoring. Servers should be prioritized according to their impact on the business or operations if they are unavailable. For example, a messaging service may be the communication backbone to your operation; in this case your monitoring should not only extend to the e-mail server, but also the domain controllers and any other servers required for the service.

## Phase 3: Evaluate and Plan

The Evaluate and Plan Phase looks at the requirements for availability monitoring of the servers in the defined critical services. In this phase, you evaluate the technology options, decide which solution to implement, test, and plan for deployment.

The first step prior to evaluating a technology solution is establishing what you need to monitor, and deriving a Health Model. The Health Model defines what it means for a system or service to be healthy (operating within normal conditions) or unhealthy (failed or degraded) and the transitions in and out of such states. Good information on a system’s health is necessary for the maintenance and diagnosis of running systems. For more information, see [Microsoft Operations Framework Service Monitoring and Control](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsmc.mspx).

### Availability Management

Availability management addresses the design, implementation, measurement, and management of IT infrastructure availability to ensure that stated business requirements for availability are consistently met. Availability management can be applied to IT services that are defined as critical business functions, even when no service level agreement exists, as is common in the Standardized level of optimization. For more information, see [Microsoft Operations Framework Availability Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx).

### 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. Software for monitoring availability of servers should have the following functionality:

* Ability to gather server attribute information, and 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.

### Response to Events

You can use the monitoring data to quantify, evaluate, and sustain a high level of IT service. This level of service is based on:

* Availability – Monitor the availability of servers by communicating with them to make sure they are running.
* Performance – Monitor performance counters to make sure that servers are running within acceptable parameters.
* Capacity – Monitor disk capacity, and capacity analysis and planning.
* Error recognition – Identify errors or conditions that affect the previous three aspects of service levels.

For information on setting availability goals, go to <http://technet.microsoft.com/en-us/library/a4bb7ca6-5a62-442e-86db-c43b6d7665a4.aspx>.

### Monitoring Data

During server monitoring, data is generated and stored in a database. Monitoring produces four types of data: event data, performance data, alert data, and discovery data.

#### Event Data

Managed servers log events into local event logs (application, security, and system). MOM, for example, collects event information from these logs. The collected event data can be used to:

* Generate reports using the Reporting Server and Reporting Database.
* Provide a context for problems that are detected (in the form of alerts).
* Provide information about computer state, which is derived from correlating data from consolidation events or missing events.

#### Performance Data

Numeric performance data is gathered from sources such as Windows performance counters and Windows Management Instrumentation (WMI). The collected performance data can be used to:

* View performance data in the Operator console using different formats such as forms, lists, and graphs.
* Generate reports using the Reporting Server and Reporting Database.
* Identify critical threshold crossings that may indicate performance issues.

#### Alert Data

Alert data represents a problem that is detected on managed servers. Alert data contains the following information about a detected problem:

* The type of entity the problem is about. This is described as a service discovery type.
* The entity the problem is about.
* The severity of the problem.
* The alert name, description, problem state, alert count, and resolution state.

Alerts are indicators that inform users about the health of managed computers. Alerts also provide the basis for status monitoring.

##### Alert Updates

Alert data that is stored in the database is continuously updated as information is collected about the server that generated the alert. Again, using MOM as an example, when a problem is detected, an alert is generated. The alert is inserted into the database as an alert that represents a new problem. If MOM detects that the problem has disappeared, it generates another alert item to update the problem state of the original alert. Eventually, the problem state of the existing alert in the database is updated and flagged as fixed; however, you still have to acknowledge the alert by resolving it.

##### Alert Suppression

Alert suppression is the mechanism for specifying which alerts should be considered as unique problems. As part of the rule definition that generates the alert, alert suppression fields are defined. If alert suppression is not set, every new alert generated by the MOM run time is treated as a new problem. Alert suppression fields are used to specify the alert properties, whose value should be identical if two alerts represent the same problem.

#### Discovery Data

Discovery data contains a snapshot of the entities discovered for a particular scope. Unlike the other operations data, discovery data is not directly exposed to the user. Discovery data is exposed as topology diagrams, computer attributes, services list, or computer lists.

## Phase 4: Deploy

After you have defined the services critical for monitoring, determined the devices required for the service, developed a Health Model, and evaluated monitoring software appropriate for your organization’s needs, 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) at Microsoft TechNet.

## Operations

The Operations goal is to manage the activities of the availability management process for critical servers. The operations process should ensure that critical IT services deliver the levels of availability defined for the organization.

## Further Information

* For more information on monitoring server availability with MOM, 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, 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>.

# *Checkpoint: Availability Monitoring of Critical Servers*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed availability monitoring software such as Microsoft Operations Manager (MOM). |
|  | Are monitoring 80 percent of your critical servers for performance, events, and alerts. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Availability Monitoring of Critical Servers.

We recommend that you follow additional best practices detailed at the [Microsoft Operations Manager 2005 TechCenter](http://www.microsoft.com/technet/prodtechnol/mom/mom2005/default.mspx) at Microsoft [TechNet](http://www.microsoft.com/technet).

Go to the [next Self-Assessment question](#_Do_you_have_9).

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 Standardized level in Data Protection and Recovery.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  No standard data management policy, which creates isolated islands of data throughout the network on file shares, nonstandard servers, personal profiles, Web sites, and local PCs  Poor or non-existent archiving and backup services makes achieving regulatory compliance difficult  Lack of disaster recovery plan could result in loss of data and critical systems  **IT Challenges**  Hardware failure or corruption equates to catastrophic data loss  Server administration is expensive  IT lacks tools for backup and restore management | **Projects**  Implement backup and restore solutions for critical servers  Consolidate and migrate file and print servers to simplify backup and restoration  Deploy data protection tools for critical servers | **Business Benefits**  Effective data management strategy drives stability in the organization and improves productivity  Standards for data management enable policy enforcement and define SLAs, improving the business relationship to IT  Strategic approach to data management enables better data recovery procedures, supporting the business with a robust platform  Organization is closer to implementing regulatory compliance  **IT Benefits**  Mission-critical application data are kept in a safe place outside of the IT location  Basic policies have been established to guarantee access to physical media (tapes, optical devices) when necessary |

The Standardized Level in the Infrastructure Optimization Model addresses key areas of Data Protection and Recovery, including Defined Backup and Restore Services for Critical Servers. It requires that your organization has procedures and tools in place to manage backup and recovery of data on critical servers.

# Requirement: Defined Backup and Restore Services for Critical Servers

## Audience

You should read this section if you do not have a backup and restore solution for 80 percent or more of your critical servers.

## Overview

Backup and recovery technologies provide a cornerstone of data protection strategies that help organizations meet their requirements for data availability and accessibility. Storing, restoring, and recovering data are key storage management operational activities surrounding one of the most important business assets: corporate data.

Data centers can use redundant components and fault tolerance technologies (such as server clustering, software mirroring, and hardware mirroring) to replicate crucial data to ensure high availability. However, these technologies alone cannot solve issues caused by data corruption or deletion, which can occur due to application bugs, viruses, security breaches, or user errors.

There may also be a requirement for retaining information in an archival form, such as for industry or legal auditing reasons; this requirement may extend to transactional data, documents, and collaborative information such as e-mail. Therefore, it is necessary to have a data protection strategy that includes a comprehensive backup and recovery scheme to protect data from any kind of unplanned outage or disaster, or to meet industry requirements for data retention.

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).

## Phase 1: Assess

The Assess Phase examines the business need for backup and recovery and takes inventory of the current backup and recovery processes in place. Backup activities ensure that data are 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 goal of the Identify Phase of your backup and recovery solution is to identify the targeted data repositories and prioritize the critical nature of the data. Critical data should be defined as data required for keeping the business running and to comply with applicable laws or regulations. 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 service level agreements (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.

While the backup and restoring of all organizational data is important, this topic addresses the backup and restore policies and procedures you must implement for critical services to successfully move from a Basic level to a Standardized level.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan Phase, 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.

#### Backup Modes

The backup mode determines how the backup is carried out in relation to the data that is being backed up. There are two ways in which data backups can take place:

Online Backups. Backups are made while data is still accessible to users.

Offline Backups. Backups are made of data that is first rendered inaccessible to users.

#### Backup Types

Various types of backups can be used for online and offline backups. An individual environment’s SLA, backup window, and recovery time requirement determine which method or combination of methods is optimal for that environment.

Full Backup. Captures all files on all disks.

Incremental Backup. Captures files that have been added or changed since the last incremental backup.

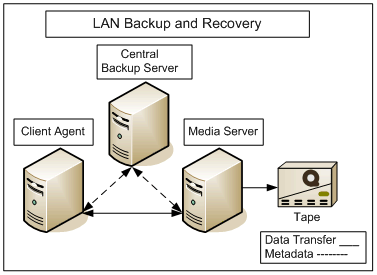
Differential Backup. Captures files that have been added or changed since the last full backup.

#### Backup Topologies

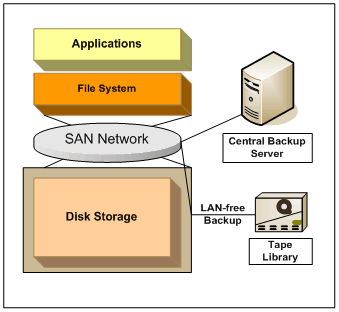
Originally, the only type of storage technology that required backup involved hard disks connected directly to storage adapters on servers. Today, this kind of storage is known as direct-attached storage, or DAS. The backup and recovery landscape has changed markedly with the development of technologies such as Storage Area Network (SAN) and Network Attached Storage (NAS). SAN environments in particular provide a significant opportunity to optimize and simplify the backup and recovery process.

Local Server Backup and Recovery (DAS). Each server is connected to its own backup device.

LAN-Based Backup and Recovery (NAS). This is a multi-tier architecture in which some backup servers kick off jobs and collect metadata about the backed-up data (also known as control data) while other servers (designated as media servers) perform the actual job of managing the data being backed up.



SAN-Based Backup and Recovery. In this topology you have the ability to move the actual backup copy operation from the production host to a secondary host system.



#### Service Plan

You have to consider many factors when designing your backup and recovery service. Among the factors to consider are:

* Fast backup and fast recovery priorities – Recovery Time Objective (RTO).
* The frequency with which data changes.
* Time constraints on the backup operation.
* Storage media.
* Data retention requirements.
* Currency of recovered data – Recovery Point Objective (RPO).

For more information on RTO and RPO, go to <http://www.microsoft.com/technet/technetmag/issues/2006/10/FailoverClusters/>.

### 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

Verifying backups is a critical step in disaster recovery. You can't recover data unless you have a valid backup.

#### Back Up Existing Log Files Before Performing Any Restoration

A good safeguard is to back up any existing log files before you restore a server. If data is lost or an older backup set is restored by mistake, the logs help you recover.

#### Perform a Periodic Fire Drill

A drill measures your ability to recover from a disaster and certifies your disaster recovery plans. Create a test environment and attempt a complete recovery of data. Be sure to use data from production backups, and to record how long it takes to recover the data. This includes retrieving data from off-site storage.

#### Create a Disaster Kit

Plan ahead by building a disaster kit that includes an operating system configuration sheet, a hard disk partition configuration sheet, a redundant array of independent disks (RAID) configuration, a hardware configuration sheet, and so forth. This material is easy enough to compile, and it can minimize recovery time—much of which can be spent trying to locate information or disks needed to configure the recovery system.

## 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.

## Operations

Monitoring and managing storage management resources for backup and recovery used in the production environment are extremely important tasks. Whether the process is centralized or distributed, the technologies and procedures for backup and recovery must be managed. In the end, the capability to easily monitor and analyze the storage management systems availability, capacity, and performance should be available.

Storage resource management (SRM) is a key storage management activity focused on ensuring that important storage devices, such as disks, are formatted and installed with the appropriate files systems.

Typically, the tools used in the production environment to monitor and manage storage resources consist of functions provided as part of installed operating systems and/or those offered with other solutions, such as [Microsoft Data Protection Manager](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/default.mspx?mfr=true).

Using a storage resource management system requires proper training and skills. An understanding of some of the basic concepts necessary for monitoring and managing storage resources successfully, and analyzing the results, is required. In addition, selecting the right tool for the right job increases the operations group’s ability to ensure data and storage resource availability, capacity, and performance.

## Further Information

* For more information on backup and recovery solutions, go to 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 achieves high server availability, go to <https://www.microsoft.com/technet/itshowcase/content/highavailcomp.mspx>.

# *Checkpoint: Defined Backup and Restore Services for Critical Servers*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Created a data backup plan and a recovery plan for 80 percent or more of your critical servers. |
|  | Used drills to test your plans. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Defined Backup and Restore Services for Critical Servers.

We recommend that you follow additional best practices addressed in the [[Backup and Recovery Services Implementation Guides](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx)](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx) of the [Windows Server System Reference Architecture](http://www.microsoft.com/wssra) and [Microsoft Operations Framework Storage Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfstomg.mspx).

Go to the [next Self-Assessment question](#_Do_you_have_10).

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 Standardized level in Security Process.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Systems are complex, incompatible, expensive, and provide limited services throughout the organization  **IT Challenges**  No consistent or secure remote or Web-based services  Lack of standard security policies  Inconsistent identification of devices connected to the network  Few IT policies and automated processes in place | **Projects**  Develop consistent processes to identify and update security issues on all devices connected to the network  Develop consistent security policy compliance on all devices connected to the network  Update to recent versions of OS and infrastructure  Plan to evaluate current software to ensure it meets security requirements | **Business Benefits**  End users have a known service level agreement and contact for troubleshoot problems, improving workforce productivity  **IT Benefits**  Security risk levels are known and managed  Incident response in more predictable and efficient  Data and devices are more secure through proactive security measures |

The Standardized level of optimization requires that your organization has defined procedures for risk management, incident management and response, and application testing.

# Requirement: Security Policies, Risk Assessment, Incident Response, and Data Security

## 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.

## 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, regional laws, or 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 your 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 Standardized level of optimization highlights specific areas of improvement.

### Security Policies

To establish an effective set of security policies and controls you need to determine the vulnerabilities that exist in your computer systems and review the security policies and controls that guard them. This review should cover areas where policies are lacking, in addition to examining current policies. Some of these areas are:

* Physical computer security policies such as physical access controls.
* Network security policies (for example, e-mail and Internet policies).
* Data security policies (access control and integrity controls).
* Contingency and disaster recovery plans and tests.
* Computer security awareness and training.
* Computer security management and coordination policies.
* Compliance of acquired software.

Your organization should have a person dedicated to reviewing and maintaining the security policies and setting the security strategy of the organization.

For detailed information on developing security policies, go to <http://www.microsoft.com/technet/security/bestprac/bpent/sec1/secstrat.mspx>.

### Risk Assessment

With a formal security risk management process, enterprises can operate in the most cost-efficient manner, with a known and acceptable level of business risk. A formal security risk management process also gives organizations a consistent, clear path to organize and prioritize limited resources to manage risk. You will realize the benefits of using security risk management when you implement cost-effective controls that lower risk to an acceptable level.

Many methodologies for prioritizing or assessing risks exist, but most are based on one of two approaches, or a combination of the two:

* Quantitative risk assessment
* Qualitative risk assessment

#### Quantitative Risk Assessment

In quantitative risk assessments, you estimate the true value of each business asset in terms of the cost of replacing it, the cost of lost productivity, the cost in respect to brand reputation, and other direct and indirect business values. From this analysis you can derive the following:

* Assigned monetary value for assets.
* A comprehensive list of significant threats.
* The probability of each threat occurring.
* The loss potential for the company on a per-threat basis over 12 months.
* Recommended safeguards, controls, and actions.

#### Qualitative Risk Assessment

Qualitative risk assessment is usually conducted through a combination of questionnaires and collaborative workshops involving people from a variety of groups within the organization; for example, information security experts, information technology managers and staff, business asset owners and users, and senior managers.

In the workshops, participants identify assets and estimate their relative value. Next they try to predict what threats each asset might be facing, and then they try to imagine what types of vulnerabilities those threats might exploit in the future. Information security experts and system administrators typically come up with controls to mitigate the risks for the group to consider and the approximate cost of each control.

Finally, the results are presented to management for consideration during a cost-benefit analysis.

For detailed information on these approaches to risk assessment, go to <http://www.microsoft.com/technet/security/guidance/complianceandpolicies/secrisk/srsgch01.mspx>.

### Incident Response

When a security event occurs, IT professionals might feel like the only things they have time to do are to contain the situation, figure out what happened, and fix the affected systems as quickly as possible. Some might try to identify the root cause, but even that might seem like a luxury under extreme resource constraints. While this kind of reactive approach can be an effective tactic, imposing a small degree of order to the reactive approach can help organizations of all types to better use their resources. With proper planning, your organization can be proactive in addressing breaches of security.

#### Reactive Approach

You must address every security incident to minimize the effect on your organization and its data. The following steps can help you manage security incidents quickly and effectively.

1. **Protect human life and people’s safety.**   
   If the affected computers control life-support equipment, shutting them down may not be an option.
2. **Contain the damage.**  
   Protect important data, software, and hardware quickly. Isolating affected computers and servers may cause a disruption of computing services, but keeping the systems up may cause widespread damage. You must rely on your judgment. Having an existing risk assessment policy in place will make the decisions easier.
3. **Assess the damage.**  
   Immediately make a duplicate of the hard disks in any servers that were attacked and put those aside for forensic use later. Then assess the damage. You should begin to determine the extent of the damage that the attack caused as soon as possible, right after you contain the situation and duplicate the hard disks.
4. **Determine the cause of the damage.**  
   To ascertain the origin of the assault, it is necessary to understand the resources at which the attack was aimed and what vulnerabilities were exploited to gain access or disrupt services. Review the system configuration, patch level, system logs, audit logs, and audit trails on the systems that were directly affected and on network devices that route traffic to them.
5. **Repair the damage.**  
   In most cases, it is very important that the damage be repaired as quickly as possible to restore normal business operations and recover data lost during the attack. The organization's business continuity plans and procedures should cover the restoration strategy.
6. **Review response and update policies.**  
   After the documentation and recovery phases are complete, you should review the process thoroughly. Determine with your team the steps that were executed successfully and what mistakes were made.

#### Proactive Approach

Proactive security risk management has many advantages over a reactive approach. Instead of waiting for bad things to happen and then responding to them afterward, you minimize the possibility of bad things ever occurring in the first place. You make plans to protect your organization's important assets by implementing controls that reduce the risk of vulnerabilities being exploited by malicious software, attackers, or accidental misuse.

An effective proactive approach can help organizations significantly reduce the number of security incidents that arise in the future, but it is not likely that such problems will completely disappear. Therefore, organizations should continue to improve their incident response processes while simultaneously developing long-term proactive approaches.

In developing a response plan you must address reactive and proactive scenarios. The reactive steps previously listed must be supplemented with proactive planning. The main areas to address in preparing a proactive approach are:

* Identify business assets.
* Determine what damage an attack against an asset could cause to the organization.
* Identify the security vulnerabilities that the attack could exploit.
* Determine how to minimize the risk of attack by implementing appropriate controls.

### Data Security

One of the most important tasks of the IT department is ensuring the security of company data. There are several steps you can take to move to the Standardized level for data security.

* You should implement antivirus controls on all computers. (See the section "Antivirus for Desktops" earlier in this guide).
* Your organization needs to establish consistent policies for classifying sensitive data.
* You need consistent processes to identify security issues and threats that could compromise sensitive company data.

For a full discussion of data security, visit <http://www.microsoft.com/technet/security/bestprac/bpent/sec3/datasec.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 an incident response plan, go to <http://www.microsoft.com/technet/security/guidance/disasterrecovery/responding_sec_incidents.mspx>.

# *Checkpoint: Security Policies, Risk Assessment, Incident Response, and Data Security*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Named a dedicated person for security strategy and policy. |
|  | Established a risk assessment methodology. |
|  | Established an incident response plan. |
|  | Established a process to manage user, device, and service identities. |
|  | Established consistent processes to identify security issues, including all network-connected devices. |
|  | Established consistent security policy compliance on network devices. |
|  | Established a consistent policy to classify data. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Standardized level for Security Policy, Risk Assessment, Incident Response, and Data Security.

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](#_Do_you_have_11).

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 Standardized level in ITIL/COBIT-Based Management Process.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Systems are complex, incompatible, expensive, and provide limited services throughout the organization  **IT Challenges**  Few IT policies and automated processes in place  Multiple hardware and software configurations  Reactive support, incident, and problem management procedures  No asset life-cycle management strategy  Lack of change or release management processes | **Projects**  Evaluate current operations framework with a self-assessment tool  Validate change preparation with release readiness practices  Define incident and problem management procedures  Develop and implement a comprehensive help desk strategy | **Business Benefits**  End users have a known service level agreement and contact for troubleshoot problems, improving workforce productivity  Changes are easier to implement due to known, repeatable processes  **IT Benefits**  IT operations are documented and understood by IT staff and the business organization  Simple configuration management improves IT operational efficiency and future deployment activities |

The Standardized level of optimization requires that your organization has defined procedures for incident management, problem management, user support, configuration management, and change management.

# Requirement: Support and Change Management Process

## Audience

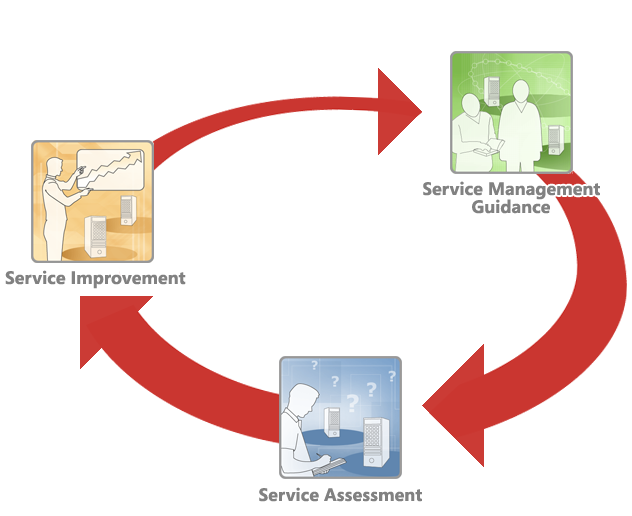
You should read this section if you do not have a process for problem, incident, service, configuration, and change management.

## 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. The [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).



The MOF Service Management Assessment is focused on enhancing the performance of people and IT service management processes, and 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 Standardized Level

The recommendations in this section are based on common issues found at the Basic level and areas of improvement sought by the Standardized level. These are only recommendations and may be different for your specific organization or industry.

At the Basic level, a large amount of time is typically spent managing problems or servicing requests. As IT service management moves into a Standardized level, problems and requests are prioritized and increasingly managed with tools. Although not formalized in policy, acceptable service levels are communicated and maintained and users know who to contact for IT services. Additionally, team roles, responsibilities, and areas of operational ownership are defined.

The Standardized level implies an increased use of tools to manage and monitor IT operations and infrastructure. Likewise, processes for change management, configuration management, and release management become standardized and predictable. Notably, predeployment testing and stabilizing becomes a priority. The Standardized level also implies an increased aptitude for project management, but there are still opportunities to improve integration of multiple, simultaneous projects and initiatives.

Microsoft provides the [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: Changing, Operating, Supporting, and Optimizing. This guide highlights areas to improve typically found in organizations at the Basic level of optimization:

* Incident Management
* Problem Management
* Improving End-User Support Services
* Service Definition and Configuration Management
* Implementing Change Management Best Practices

Depending on the organization, improvements to these 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.

### Incident Management

[Incident management](http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfincmg.mspx) is a critical process that provides organizations with the ability to first detect incidents, and then target the correct support to resolve the incidents as quickly as possible.

The primary goal of incident management is to restore normal service operation as quickly as possible and to minimize the adverse impact on business operations to maintain the best possible levels of service quality and availability. Normal service operation is defined as a service operation within service level agreement (SLA) limits.

The objectives of incident management are:

* To restore normal service as quickly as possible.
* To minimize the impact of incidents on the business.
* To ensure that incidents and service requests are processed consistently and that none are lost.
* To direct support resources where most required.
* To provide information that allows support processes to be optimized, the number of incidents to be reduced, and management planning to be carried out.

The following sections discuss the major processes within incident management.

## Phase 4: Deploy (Incident Management)

#### Detection, Self-Service, and Recording

The detection process records incidents through a variety of mediums, including those reported by people contacting the Service Desk, or incidents raised by alerts in event management systems.

End users may access self-service facilities to raise their own incidents, check progress on existing incidents, and access self-help information.

All incidents must be recorded, so that they can be tracked, monitored, and updated throughout their life cycle. This information can then be used for problem management, reporting, process optimization, and planning purposes.

#### Service Request Handling

This process defines the handling of service requests. Different types of service requests must be handled in different ways. The Service Desk may be able to process certain requests, while other requests need to be passed to other teams, such as change management, for processing.

#### Classification and Initial Support

The classification process categorizes the incident by assigning a priority.

The initial support process provides a first-line resolution for incidents. This can be achieved by checking them against known errors, existing problems, and previous incidents to identify documented workarounds.

#### Investigation and Diagnosis

This process deals with investigation of the incident and gathering of diagnostic data to identify how the incident can be resolved as quickly as possible. The process includes escalation to higher management or to technical expertise, and functional escalation if necessary to meet SLA targets.

#### Major Incident Procedure

The major incident procedure addresses critical incidents that require a response above and beyond that provided by the normal incident process. Such incidents may have a major impact on the ability to sustain operations or effectively run the business. Although these incidents still follow the normal incident life cycle, the major incident procedure provides the increased coordination, escalation, communication, and resources that these high-priority events require.

#### Resolution and Recovery

The resolution and recovery process covers the steps required to resolve the incident, often by interfacing with the change management process to implement remedial actions. After actions have been taken, the success of the resolution is verified.

Following resolution of the incident, such as replacement of a faulty hard disk, there may be recovery actions that need to be taken, such as the restoration of data and restarting the service.

#### Problem Closure

This process ensures that the customer is satisfied that the incident has been resolved prior to closing the incident record.

### Problem Management

By implementing [problem management](http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfprbmg.mspx) processes at the same time as incident management processes, organizations can identify and resolve the root causes of any significant or recurring incidents, thus reducing the likelihood of recurrence.

The objectives of problem management are to:

* Identify and take ownership of problems affecting infrastructure and service.
* Take steps to reduce the impact of incidents and problems.
* Identify the root cause of problems and initiate activity aimed at establishing workarounds or permanent solutions to identified problems.
* Using recorded problem and incident data, perform trend analysis to predict future problems and enable prioritization of problem management activity.

The following sections discuss major processes within problem management.

## Phase 4: Deploy (Problem Management)

#### Problem Recording and Classification

This process deals with initial detection and recording of a problem. Problems may be reported through the incident management process or detected through analysis of the data collected by the problem management team. You must link problems to existing incidents and record the problem to facilitate prioritization of problem resolutions. After you have recorded a problem, you assess the impact on the business and determine the urgency of the resolution. This assessment determines the problem classification.

#### Problem Investigation and Diagnosis

This process deals with the investigation of the problem and the diagnosis of the root cause. The data can then be used to help the problem management team assess the resources and skills required to resolve the cause of the problem. The process includes dealing with major problems that require additional planning, coordination, resources, and communication, and which may result in a formal project being initiated.

#### Error Control

The error control process addresses successful correction of known errors. The objective is to change IT components or procedures to remove known errors affecting the IT infrastructure and thus prevent any recurrence of incidents.

#### Problem Closure

The problem closure process outlines the need to fully record details of all errors. It is vital to save data on the configuration items (CIs), symptoms, and resolution or circumvention actions relating to all problems. This will build up the organization’s knowledge base.

Following successful implementation of changes to resolve errors, the error record can be closed, together with any associated incident or problem records. A post-implementation review (PIR) can then confirm the effectiveness of the solution.

### Improving End-User Support Services

Support services, or the [Service Desk](http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfsvcdk.mspx) is the first point of contact for the organization. Its efficient and effective response to customer problems and concerns can do much to enhance the reputation of the company.

The objectives of the Service Desk can vary based on a number of factors, such as the size of the organization and the defined scope of the Service Desk function.

Service objectives include:

* Providing a single and central point of contact between users and the IT department.
* Providing an interface for users to other service management functions.
* Delivering the high-quality support required for achieving business goals.
* Identifying and lowering the total cost of ownership (TCO) of IT services.
* Supporting changes across business, technology, and process boundaries.
* Improving customer satisfaction.
* Retaining all customers.
* Identifying additional business opportunities.

The major processes within the Service Desk function are addressed in the following sections.

## Phase 4: Deploy (Service Desk)

#### Record and Service Incidents

An incident is a single occurrence of an event that is not part of the standard operation of a service. An incident may cause an interruption to the normal operation of a service or a reduction in the quality of that service.

The function of the Service Desk in this case is to facilitate the restoration of the service to the affected users as quickly as possible.

#### Manage Service Requests

A service request could be any one of the following examples:

* A request for change.
* A request for information (that is, a query).
* An as-needed job request.
* A procurement request.
* Any communication between a user and the IT department (for example, a complaint, compliment, comment, or suggestion).

The function of the Service Desk in the case of a service request is to ensure that the request is dealt with to the satisfaction of the user, either by satisfying the request directly or by allocating the request to an appropriate resolution group.

### Service Definition and Configuration Management

A key principle in effectively managing an IT infrastructure is to document its components and the relationships between them. [Configuration management](http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfcfgmg.mspx) provides the foundation for decision-making in change management, negotiating SLAs, assessing IT capacity, and other critical processes.

Configuration management is a critical process responsible for identifying, controlling, and tracking all versions of hardware, software, documentation, processes, procedures, and other components of the IT organization. The goal of configuration management is to ensure that only authorized components, referred to as configuration items (CIs), are used in the IT environment and that all changes to CIs are recorded and tracked throughout the component’s life cycle. The configuration management process includes the following objectives:

* Identify configuration items and their relationships and add them to the configuration management database (CMDB).
* Enable access to the CMDB and CIs for other functions.
* Update and change CIs following changes to IT components during the release management process.
* Establish a review process that ensures that the CMDB accurately reflects the production IT environment.

The following sections discuss the objectives of configuration management.

## Phase 4: Deploy (Configuration Management)

#### Establish Configuration Items (CIs)

As you design the CMDB, you need to determine an appropriate level of detail for each CI. Then each CI in your organization can be added to the CMDB.

One of the key benefits configuration management provides, in addition to asset management, is the modeling of relationships between IT components. For example, a workstation is made up of a desktop computer, operating system, and applications, and the workstation is connected to and uses the network. The proper understanding and documentation of relationships between IT components makes it possible to perform detailed impact analysis on a proposed change.

#### Access Configuration Items

After you have added information about IT components and relationships to the CMDB, the information can then be used by other SMFs. Change management, for example, uses the relationships defined within the CMDB to determine the impact of a change on other components within the IT environment.

#### Change Configuration Items

As release management begins to make changes to IT components, corresponding changes must be made to the CMDB. Without accurate and up-to-date information, the value of configuration management is lost. This process should be done automatically wherever possible. The amount of information and the frequency of change make manual data entry impractical for all but the smallest organizations.

#### Review Configuration Items

The accuracy of the information stored in the CMDB is crucial to the success of the Change Management and Incident Management SMFs, as well as other service management functions. A review process that ensures that the database accurately reflects the production IT environment needs to be established.

### Implementing Change Management Best Practices

[Change management](http://www.microsoft.com/technet/itsolutions/cits/mo/smf/smfchgmg.mspx) describes a consistent set of processes to initiate infrastructure changes, assess and document their potential impacts, approve their implementation, and schedule and review their deployment.

The goal of change management is to provide a disciplined process for introducing required changes into the IT environment with minimal disruption to ongoing operations. To achieve this goal, the change management process includes the following objectives:

* Formally initiate a change through the submission of a request for change (RFC).
* Assign a priority and a category to the change after assessing its urgency and its impact on the infrastructure or end users.
* Establish an efficient process for passing the RFC to decision makers for approval or rejection of the change.
* Plan the deployment of the change.
* Work with release management to manage the release and deployment of changes into the production environment. For more information about the MOF Release Management SMF, go to <http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfrelmg.mspx>.
* Conduct a post-implementation review to determine whether the change has achieved its goals and determine whether to keep the change or to reverse it.

The following sections discuss the objectives of configuration management.

## Phase 4: Deploy (Change Management)

#### Process Change Requests

Typically, any person within a business environment can request a change and, by doing so, become a change initiator. Because the pool of potential change initiators is large and consists of people with varying degrees of familiarity with the procedures involved, a process is required that produces change requests of consistent quality and completeness and discards irrelevant requests.

#### Assign Change Classification to Accepted Change Requests

At this stage, the change request has passed the initial screening, although it has not yet been approved. The next requirement is to classify the priority and category of the change. Even though the priority and classification have been entered by the change initiator, the change manager or a designated deputy reviews them and has the authority to change them if necessary.

#### Change Authorization

After a change has been correctly prioritized and categorized by the change manager, the change must be authorized.

#### Change Development

After an RFC has been approved (using the appropriate path based on its priority and category), it moves into the change development phase. This phase addresses the steps necessary to plan the change, develop the deliverables of the change (for example, developing new code or configuring new hardware), and the handover to the release management process for the deployment of the change into the production environment.

#### Change Review

Following a successful release and deployment into the production environment or, as in the case of a standard change, a deployment into production, a review process must be conducted to establish whether the change has had the desired effect and has met the requirements from the original request for change.

## Recommended Reading

[MOF Supporting Quadrant](http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofsupport.mspx)

[MOF Changing Quadrant](http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofchange.mspx)

# *Checkpoint: Support and Change Management Process*

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented incident management techniques. |
|  | Implemented problem management techniques. |
|  | Improved end-user support services. |
|  | Implemented service definition and configuration management |
|  | Implemented change management best practices. |

If you have completed the step listed above, your organization has met the minimum requirement of the Standardized level for Support and Change Management Processes in the ITIL/COBIT-Based Management Process capabilities of the Infrastructure Optimization Model.

We recommend that you follow additional best practices found in the [Supporting](http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofsupport.mspx) and [Changing](http://www.microsoft.com/technet/itsolutions/cits/mo/mof/mofchange.mspx) quadrants of the [Microsoft Operations Framework](http://www.microsoft.com/mof), and to develop a base knowledge of MOF, ITIL, and COBIT concepts.

Additional Resources: Tools and Technologies

Recommended tools, technologies, and services for moving from Basic to Standardized 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. |
| [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. |
| [Microsoft Exchange Server](http://www.microsoft.com/technet/prodtechnol/exchange/default.mspx) | Exchange Server is messaging and collaboration software that enables users to send and receive e-mail and other forms of interactive communication through computer networks. |
| [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. |
| [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 corporate 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) | Windows Server 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=96674) | The Windows Vista Hardware Assessment Solution Accelerator is an assessment tool that inventories computers on a network and reports on their readiness to run the Windows Vista operating system or the 2007 Microsoft Office System. This accelerator does not require installation of agents on the computers. The auto-generated readiness reports describe whether each computer is Windows Vista Capable or Windows Vista Premium Ready (before and after hardware upgrades), and provide detailed information about the system hardware and installed devices. |

# 

Additional Resources: Basic to Standardized Checklist

The following checklist outlines the requirements you must meet to move to the Standardized level. After you have addressed each item under the main topics, you have successfully moved from the Basic level to the Standardized level.

Once you have incorporated all of the processes and technologies highlighted in this guide, your organization has reached the Standardized level. Your next step is to explore the benefits and requirements for progressing to the Rationalized level. Guidelines for moving to the Rationalized level are in the Core IO Implementer Resource Guide: Standardized to Rationalized.

## Identity and Access Management

### Directory Services for Authentication of User

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented Active Directory directory service for authentication of 80 percent or more of connected users. |

## Desktop, Device and Server Management

### Automated Patch Distribution to Desktops and Laptops

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | 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. |

### Defined Standard Images for Desktops and Laptops

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Used tools to capture a standard image. |
|  | Defined a strategy for standard images. |
|  | Defined a standard set of disk images (OS and applications) for all hardware types. |
|  | Established deployment tools for network-based or offline image installation. |

### Centralized Management of Mobile Devices

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed software to discover and track the mobile devices in your organization |
|  | Implemented password-controlled access. |
|  | Established centralized data and software synchronization. |
|  | Ensured that decommissioned devices are free of company information. |

### Identity Validation, Data Protection, and Data Backup of Mobile Devices

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Established and are enforcing a password-access policy or using public key certificates for user identification. |
|  | Encrypted all transfers for data distribution to, and data backup from, mobile devices. |
|  | Implemented device lockout on mobile devices. |
|  | Ensured that company information can be removed with remote wipe in case a mobile device is lost or stolen. |

### Consolidation of Desktop Images to Two Operating System Versions

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented an image-consolidation strategy. |
|  | Reduced the number of production operating systems to no more than two. |

## Security and Networking

### Antivirus Software for Desktops

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed all operating system and software application security updates. |
|  | Activated available host-based firewalls. |
|  | Installed antivirus software on 80 percent or more of your desktop computers. |

### Central Firewall Services

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed a centralized hardware or software firewall. |

### Internally Managed Basic Networking Services (DNS, DHCP, WINS)

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Implemented DNS services on servers or other devices within your organization. |
|  | Implemented DHCP services on servers or other devices within your organization. |
|  | Implemented WINS services for older operating systems on servers or other devices within your organization. |

### Availability Monitoring of Critical Servers

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Installed availability monitoring software such as Microsoft Operations Manager (MOM). |
|  | Are monitoring 80 percent of your critical servers for performance, events, and alerts. |

## Data Protection and Recovery

### Defined Backup and Restore Services for Critical Servers

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Created a data backup plan and a recovery plan for 80 percent or more of your critical servers. |
|  | Used drills to test your plans. |

## Security Process

### Security Policies, Risk Assessment, Incident Response, and Data Security

|  |  |
| --- | --- |
| **X** | **Requirement** |
|  | Named a dedicated person for security strategy and policy. |
|  | Established a risk assessment methodology. |
|  | Established an incident response plan. |
|  | Established a process to manage user, device, and service identities |
|  | Established consistent processes to identify security issues, including all network-connected devices |
|  | Established consistent security policy compliance on network devices |
|  | Established a plan to evaluate and test all acquired software for security compliance |
|  | Established a consistent policy to classify data |

## ITIL/COBIT-based Management Process

### Support and Change Management Process

|  |  |
| --- | --- |
| X | Requirement |
|  | Implemented incident management techniques. |
|  | Implemented problem management techniques. |
|  | Improved end-user support services. |
|  | Implemented service definition and configuration management |
|  | Implemented change management best practices. |