

Core Infrastructure Optimization   
Implementer Resource Guide:   
Rationalized to Dynamic

Published: July 2007

Abstract

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

This is the third 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 Rationalized level to the Dynamic level.

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

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

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

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

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

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

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

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

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

Contents

[Core Infrastructure Optimization Implementer Resource Guide: Rationalized to Dynamic 1](#_Toc171967119)

[Resource Guide Overview 1](#_Toc171967120)

[Audience 1](#_Toc171967121)

[Infrastructure Optimization Concept 1](#_Toc171967122)

[Core Infrastructure Optimization Capabilities 3](#_Toc171967123)

[Core Infrastructure Optimization Model Levels 3](#_Toc171967124)

[Core Infrastructure Optimization Capability Overview 5](#_Toc171967125)

[Capability: Identity and Access Management 13](#_Toc171967126)

[Introduction 13](#_Toc171967127)

[Requirement: Centralized Automated User Account Provisioning Across Heterogeneous Systems 14](#_Toc171967128)

[Requirement: Directory-based Authentication of External Customers and Business Partners 19](#_Toc171967129)

[Capability: Desktop, Device and Server Management 27](#_Toc171967130)

[Introduction 27](#_Toc171967131)

[Requirement: Automated Infrastructure Capacity Planning for Primary IT Services 29](#_Toc171967132)

[Requirement: Management of Mobile Devices 33](#_Toc171967133)

[Requirement: Virtualization to Dynamically Move Workloads from Server to Server 37](#_Toc171967134)

[Capability: Security and Networking 43](#_Toc171967135)

[Introduction 43](#_Toc171967136)

[Requirement: Integrated Threat Management and Mitigation Across Clients and Server Edge 44](#_Toc171967137)

[**Requirement: Model-enabled Service Level Monitoring of Desktops, Applications, and Server Infrastructure** 46](#_Toc171967138)

[Requirement: Quarantine Solution for Unpatched or Infected Computers 49](#_Toc171967139)

[Capability: Data Protection and Recovery 55](#_Toc171967140)

[Requirement: Backup and Restore and Defined Recovery Times via SLA for Desktops 55](#_Toc171967141)

[Capability: Security Process 61](#_Toc171967142)

[Introduction 61](#_Toc171967143)

[Requirement: Advanced Two-Factor User Authentication 61](#_Toc171967144)

[Capability: ITIL/COBIT-based Management Process 65](#_Toc171967145)

[Introduction 65](#_Toc171967146)

[Requirement: Optimizing Processes 65](#_Toc171967147)

[Additional Resources: Tools and Technologies 79](#_Toc171967148)

[Additional Resources: Rationalized to Dynamic Checklist 83](#_Toc171967149)

Core Infrastructure Optimization   
Implementer Resource Guide:   
Rationalized to Dynamic

This document provides a technology roadmap for implementing 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.

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 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 |
| 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 Rationalized level of IT infrastructure and processes to the Dynamic level in the Core Infrastructure Optimization Model. Other resource guides in this series focus on the capabilities necessary to move from lower levels in the Core Infrastructure Optimization Model.

# Core Infrastructure Optimization Capabilities

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

## Identity and Access Management

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

## Desktop, Device and Server Management

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

## 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.

## 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.

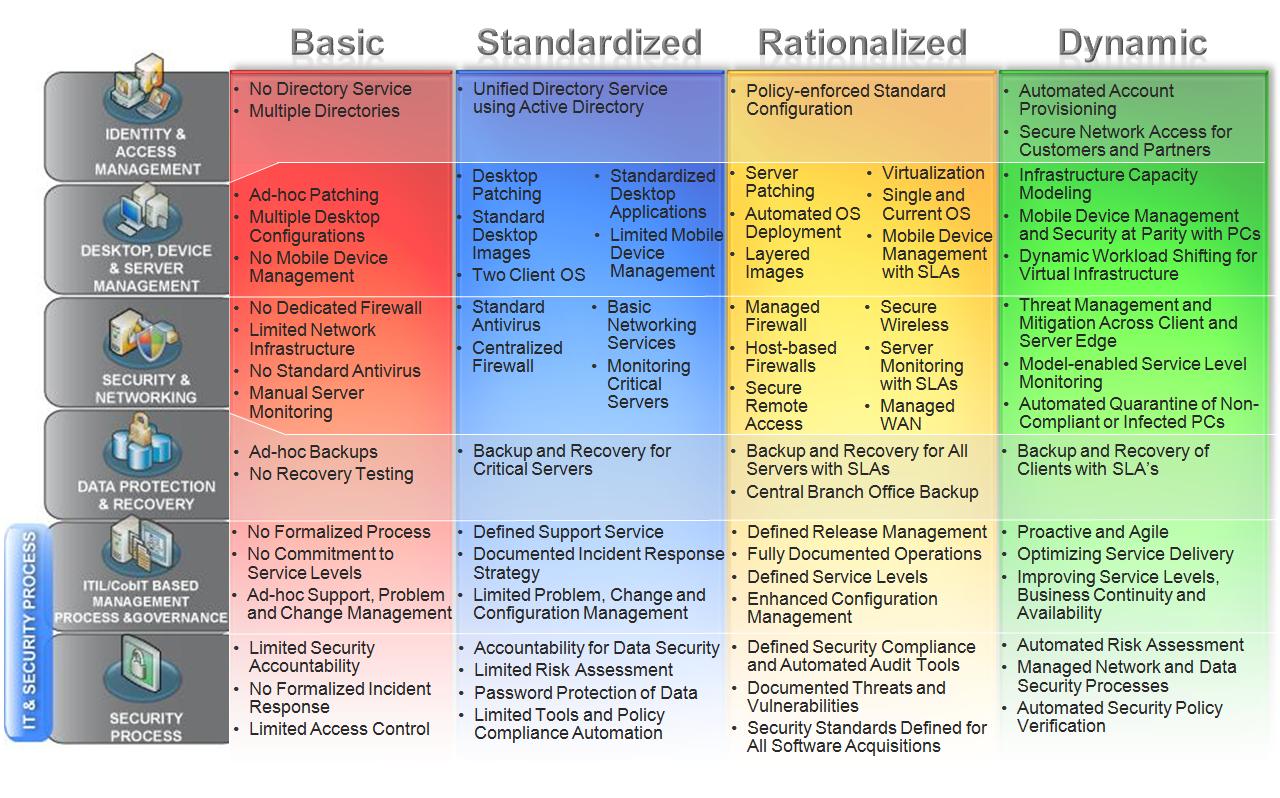


Figure 1. Capability requirements of each optimization level

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

## Self Assessment

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

The following section presents questions for each of the core capabilities that direct you to relevant sections of this planning guide. Your answers to the questions will dictate which sections contain guidance applicable to your organization. Many requirements in the following section have minimum attributes associated with them. If your organization meets every requirement and requirement attribute outlined in this section, you have already achieved the Dynamic level. At this point, your organization will have implemented continuous improvement methodologies to determine how to reach further levels of organizational maturity beyond the Dynamic level in your IT organization. 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 Dynamic level of optimization requires centrally managed user provisioning across heterogeneous similar systems, as well as federated identity management across organizational and platform boundaries. By moving to the Dynamic level, this guide assumes the requirements for the Rationalized level have already been met, including the presence of directory-based tools and procedures for enforcement of desktop and server configuration and security policies, information protection procedures and infrastructure in place, and managed local policy and security templates implemented on desktops.

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Centralized automated user account provisioning (for example, issuing new accounts, changing passwords, synchronizing permissions, or enabling access to business applications) across 80 percent or more of heterogeneous systems. |  |  |
| Attributes:   * Defined current identity object provisioning workflows in your organization, as well as areas to improve or optimize. * Identified technologies used to manage object identity life cycles. * Implemented a consolidated solution to automate common user account provisioning workflows. | | |

For more details, see [automated user account provisioning](#_Requirement:__Centralized) in this document, or visit the following Web sites:

* [Provisioning and Workflow in the Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2prov_6.mspx)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Identity and Access Management | Yes | No |
| Implemented a federated directory-based tool to enable authenticated access to external customers, service providers, and business partners. |  |  |
| Attributes:   * Validated need for providing authenticated access to external entities. * Determined strategies and policies for providing external access to defined resources. * Implemented technologies to ensure secure access for defined external users to defined services. | | |

For more details, see [federated directory-based services to authenticate external users](#_Requirement:_Directory-based_Authen) 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)
* [Active Directory Federation Services (ADFS)](http://technet2.microsoft.com/WindowsServer/f/?en/library/1f6e9e6e-c179-4dd2-bd1d-c74dd4ebf56b1033.mspx)
* [Windows Server 2003 Technical Library](http://technet2.microsoft.com/WindowsServer/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx)
* [Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx)

### Capability: Desktop, Device and Server Management

The Dynamic level of optimization requires that your organization has procedures and tools in place to automate service management of mobile devices and to get them close to parity with desktops in regards to manageability and security. Additionally, the Dynamic level requires the use of virtualization in production for the consolidation and balancing of server workloads. By moving to the Dynamic level, this guide assumes the requirements for the Rationalized level have already been met, including automated hardware and software asset management, automated patch management to desktops and servers, automated operating system image deployment, desktop image consolidation using thin images with recent software and operating systems, and plans in place to begin using virtualization technologies in production.

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Tools in place to perform automated infrastructure capacity planning for primary IT services (such as e-mail). |  |  |
| Attributes:   * Identified primary IT service candidates for automated capacity planning. * Created capacity models to automate capacity planning or implemented capacity planning tools. | | |

For more details, see automated [infrastructure capacity planning](#_Requirement:_Automated_Infrastructu) in this document, or visit the following Web sites:

* [Capacity Management in the Microsoft Operations Framework](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcapmg.mspx)
* [Microsoft System Center Capacity Planner 2006](http://www.microsoft.com/systemcenter/sccp/overview/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Management of mobile devices and access to IT services and applications nearly at parity with managed desktop and laptop computers. |  |  |
| Attributes:   * Implemented secure technologies to provide access to primary line-of-business applications (for example, LOB apps, CRM, or supply chain) via mobile devices. * Established defined set of standard basic images for mobile devices. * Implemented an automated solution to continuously update configuration settings and/or applications in mobile devices. * Deployed an automated quarantine solution for mobile devices. * Implemented an automated patch management solution for mobile devices. * Implemented an automated asset management solution for mobile devices. | | |

For more details, see [dynamic mobile device management and access](#_Requirement:_Management_of) in this document, or visit the following Web sites:

* [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 Windows Mobile Center](http://www.microsoft.com/technet/solutionaccelerators/mobile/default.mspx)
* [Windows Mobile Solutions Providers](http://www.microsoft.com/windowsmobile/resources/providers/search.asp)

|  |  |  |
| --- | --- | --- |
| Requirement: Desktop, Device and Server Management | Yes | No |
| Implemented virtualization to dynamically move workloads from server to server based on resource needs or business rules. |  |  |
| Attributes:   * Deployed a subset of production IT services or applications to virtual machines. * Actively managing and optimizing system resources on shared hardware devices. | | |

For more details, see [implementing virtualization](#_Requirement:_Virtualization_to) in this document, or visit the following Web sites:

* [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx)
* [Implementation Guide in the Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaimg.mspx)
* [Microsoft Virtual Server 2005 R2 on TechNet](http://www.microsoft.com/technet/prodtechnol/virtualserver/default.mspx)
* [System Center Virtual Machine Manager 2007](http://www.microsoft.com/systemcenter/scvmm/default.mspx)

### Capability: Security and Networking

The Dynamic level of optimization requires that your organization has implemented integrated threat management and mitigation across client and server edge, true service level monitoring of defined services extending from the data center to end users, and a quarantine solution for unpatched or infected computers. By moving to the Dynamic level, this guide assumes the requirements for the Rationalized level have already been met, including policy-managed local firewalls on servers and desktops, secure wireless network deployed, IPsec solution implemented, public key infrastructure (PKI) and certificate services in place, as well as secure remote access via virtual private networks (VPNs) and optimized wide area network (WAN) links to branch offices.

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Integrated threat management and mitigation across clients and server edge. |  |  |
| Attributes:   * Assessed server edge security threats and evaluated threat mitigation solutions. * Implemented technology solutions to protect against Internet-based threats across the client and server edge. | | |

For more details, see [threat management and mitigation](#_Requirement:_Integrated_Threat) in this document, or visit the following Web sites:

* [ISA Server TechCenter on Microsoft TechNet](http://www.microsoft.com/technet/isa/default.mspx)
* [Microsoft’s Intelligent Application Gateway (IAG) 2007](http://www.microsoft.com/forefront/edgesecurity/iag/overview.mspx)
* [Windows Server System Reference Architecture Firewall Services Implementation Guide](http://www.microsoft.com/technet/itsolutions/wssra/raguide/firewallservices/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Model-enabled service level monitoring of desktops, applications, and server infrastructure. |  |  |
| Attributes:   * Defined desktop, application, and server infrastructure service models. * Evaluated technologies for monitoring availability of connections and components across defined services. * Implemented automated solution to define and monitor service levels. | | |

For more details, see [model-enabled service level monitoring](#_Requirement:_Model-enabled_Service) in this document, or visit the following Web sites:

* [System Center Operations Manager 2007 on Microsoft TechNet](http://www.microsoft.com/technet/opsmgr/default.mspx)
* [Operations Manager 2007 Online Help and Document Library](http://technet.microsoft.com/en-us/library/bb381239.aspx)
* [Service Level Management in Microsoft Operations Framework](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and Networking | Yes | No |
| Automated quarantine solution for unpatched or infected computers. |  |  |
| Attributes:   * Evaluated technologies to enable network quarantine for remote and on-site users. * Implemented VPN quarantine solution for remote users. | | |

For more details, see [automated quarantine services](#_Requirement:_Quarantine_Solution) in this document, or visit the following Web sites:

* [Implementing Quarantine Services with Microsoft Virtual Private Network Planning Guide on Microsoft TechNet](http://www.microsoft.com/technet/security/prodtech/windowsserver2003/quarantineservices/default.mspx)
* [Network Access Quarantine Control in Windows Server 2003 Guide](http://www.microsoft.com/technet/network/vpn/quarantine.mspx)
* [Virtual Private Networks Web site on Microsoft TechNet](http://www.microsoft.com/technet/network/vpn/default.mspx)

### Capability: Data Protection and Recovery

The Dynamic level of optimization requires that your organization has procedures and tools in place to manage backup and recovery of data on desktops. By moving to the Dynamic level, this guide assumes that the requirements for the Rationalized level have already been met, including defined backup and recovery services for all managed servers in central, hub, and branch locations.

|  |  |  |
| --- | --- | --- |
| Requirement: Data Protection and Recovery | Yes | No |
| Implemented defined backup and restore services with service level agreements (SLAs) for 80 percent or more of desktops. |  |  |
| Attributes:   * Established goals for the desktop backup and recovery service. * Defined and implemented a suitable backup and restore service for desktops in the organization and established SLAs. | | |

For more details, see [managed backup for desktops](#_Requirement:_Backup_and) in this document, or visit the following Web sites:

* [Windows XP Professional Resource Kit: Backing Up and Restoring Data](http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c14621675.mspx)
* [Microsoft Data Protection Manager 2006 Planning Guide](http://www.microsoft.com/technet/prodtechnol/dpm/proddocs/57145992-e0e0-43be-837c-19a7b3b463c8.mspx)
* [Windows Server System Reference Architecture Backup and Recovery Services](http://www.microsoft.com/technet/itsolutions/wssra/raguide/backupandrecoveryservices/default.mspx)

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

The Dynamic level of optimization requires that your organization is optimizing and continually improving its delivery of IT services. At the Rationalized level, service level agreements were in place for server monitoring and backup and recovery services. At the Dynamic level, SLAs are extended to all managed IT services, and security also becomes more sophisticated with advanced two-factor authentication using biometric scans or equivalent to access highly sensitive or critical data.

|  |  |  |
| --- | --- | --- |
| Requirement: Security and ITIL/COBIT-based Management Process | Yes | No |
| Established security processes and technologies to enable advanced two-factor user authentication (such as biometric scans) for highly sensitive data. |  |  |
| Attributes:   * Developed and implemented advanced two-factor identity and access management policies for highly sensitive data. | | |

For more details, see [advanced two-factor user authentication](#_Requirement:_Advanced_Two-Factor) in this document, or visit the following Web sites:

* [The Secure Access Using Smart Cards Planning Guide](http://www.microsoft.com/technet/security/guidance/networksecurity/securesmartcards/default.mspx.)
* [Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx)

|  |  |  |
| --- | --- | --- |
| Requirement: Security and ITIL/COBIT-based Management Process | Yes | No |
| Implemented best practices for further optimizing your IT organization. |  |  |
| Attributes:   * Implemented best practice Availability Management. * Implemented best practice Financial Management. * Implemented best practice Infrastructure Engineering. * Implemented best practice IT Service Continuity Management. * Implemented best practice Workforce Management. | | |

For more details, see [optimizing processes](#_Requirement:_Operating,_Optimizing,) in this document, or visit the following Web site:

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

## Preparing to Implement Core IO Requirements

The detailed capability and requirement sections of the *Core Infrastructure Optimization Implementer Resource Guide: Rationalized to Dynamic* 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 Dynamic level. These sections provide contextual detail for areas to focus on, an introduction to processes and technologies, and links to relevant implementation guidance throughout.

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

### Phased Approach

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

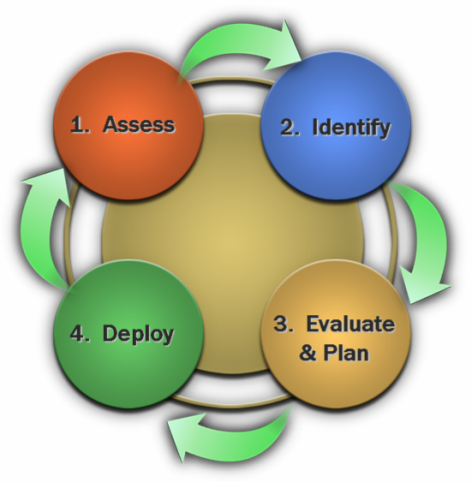


Figure 2. Four phases of the IO capabilities

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

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

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

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

### Solution Currency

The detailed Capability and Requirement sections of the *Core Infrastructure Optimization Implementer Resource Guide: Rationalized to Dynamic* 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. Some products or technologies are in the process of being released as this guidance has been written; in these cases relevant products are described in brief and hyperlinks are provided to corresponding Microsoft TechNet Web sites. Please visit [Microsoft TechNet](http://www.microsoft.com/technet) regularly for any updates to products and capabilities referred to in this document.

### Implementation Services

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

Capability: Identity and Access Management

# Introduction

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

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

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Users still require help desk to access resources—no user provisioning  No clear view of organization’s identity  **IT Challenges**  Lack of single sign-on across multiple systems although identities are centrally administered and settings and configurations are easily managed  Users continue receiving several authentication prompts daily | **Projects**  Implement solution to centrally manage user provisioning  Implement a federated identity management solution across organizational and platform boundaries | **Business Benefits**  Provide single sign-on across multiple systems reduces administration costs and increases user productivity  Various identity repositories are connected federated within firewall or trusted to allow provisioning of identity workflow  **IT Benefits**  Centralized password administration  Automated identity account de-provisioning and life-cycle management  Reduced support costs and user downtime |

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/P2Ident.mspx?mfr=true)
* Access Management and Single Sign-On
* [Intranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)
* [Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true)

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

The Standardized and Rationalized levels of Identity and Access Management in the Infrastructure Optimization Model address the key areas of a unified directory service and automated enforcement configurations and security policies. The Dynamic level extends these capabilities by implementing automated user account provisioning and secure access of network resources to third parties.

# Requirement: Centralized Automated User Account Provisioning Across Heterogeneous Systems

## Audience

You should read this section if you do not have a centralized and automated tool for user account provisioning across 80 percent or more of your heterogeneous systems.

## Overview

Today's large organizations often have complex and poorly designed processes for provisioning systems with information for computer network users. For example, in some organizations, it can take up to two weeks before new information workers can access e-mail and the applications that they need for their jobs. The manual, task-intensive processes that are typically involved in identity provisioning add overhead, delay employee productivity, and often lead to a network environment that is not secure.

The manual administration of provisioning tasks is slow and typically does not enforce policies for access and authorization in a consistent manner. Without reliable, automated processes it will often not be practical to even attempt to implement all desirable policies.

Organizations store identity information in numerous repositories, or data stores. Using a product that includes metadirectory functionality allows you to synchronize existing data so that it is consistent across these stores. To move to the Dynamic level, you need to implement and utilize technologies that allow centralized and automated provisioning.

## Phase 1: Assess

During the Assess phase, you should follow the typical activities that take place when employees join your organization, transfers or employee reorganizations occur, passwords are reset, or other self-driven common requests to user directories are made. These processes or workflows will always occur in any organization; some change workflows are more manually processed than others. The product of the Assess phase is a catalog that contains the workflows that exist to resolve common directory provisioning requests, any existing policies around access and authorization, and identification of required manual controls for change or access authorization. A record of the typical time required from initial request to change resolution will also aid in planning which tasks receive priority and can be used once the provisioning solution has been implemented to calculate productivity improvements.

## Phase 2: Identify

Once you have identified the underlying workflows, policies, and effort required to perform common user provisioning tasks, the Identify phase identifies areas of improvement for existing directories or user activities.

This document highlights three primary scenarios for conducting the Identify phase:

* HR-driven provisioning
* Group management
* Self-service provisioning

These scenarios will typically correspond with many of the challenges associated with your organization’s account provisioning and directory services, but they are not a comprehensive list. The results of this phase will be to identify many of the key areas of improvement or current policy violations to be included during the Evaluate and Plan phase of the project. Success criteria should include task-related efficiency gains as well as correction of the issues called out in the following sections.

### HR-driven Provisioning

In this scenario, synchronizing identity information is only part of the required solution. In addition to enabling a comprehensive view of your users, you need an automated provisioning solution.

HR-driven provisioning addresses and corrects these issues:

* Duplicated effort maintaining disparate data stores
* Inconsistent data
* Users “borrowing” another’s account
* Stale accounts (those not promptly disabled or removed)
* Inappropriate access

### Group Management

Organizations typically use distribution groups to distribute e-mail and security groups to conveniently group users with similar entitlements. The challenge is to manage these different types of groups to ensure that the correct entitlements are granted or revoked in a timely manner in accordance with business rules, while providing the most efficient e-mail routing and the best user experience.

Without a centralized and automated provisioning solution, it is difficult both to place users in the appropriate groups during the provisioning process and to manage groups as users change roles, positions, and locations during their careers. This situation leads to user frustration, increased help desk call volume, and inappropriate access granted to some users.

Group management addresses and corrects these issues:

* Delayed access for new users
* Incorrect distribution lists
* Stale groups
* Redundant e-mail
* Authorizations that are not removed when an employee leaves a group
* Excessive number of administrative accounts

### Self-Service Provisioning

While HR-driven provisioning is usually considered the authoritative source for permanent employees, it is not always an authoritative data source to drive fully automated provisioning for contractors and temporary employees.

Self-service provisioning addresses and corrects these issues:

* Delays in contractors being able to do their jobs
* Stale accounts
* Inefficient or insecure password delivery
* Duplicate accounts

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, you will look at what technologies can be used to aid in automating user account provisioning and self-service. You should evaluate and compare the functionality and costs associated with the tools and their implementation. Once a technology is selected, during the planning process you should discuss the implementation of the provisioning technology and prioritize the scenarios. Microsoft provides several tools that you can use to centralize and automate user provisioning in heterogeneous computing environments:

* Microsoft Identity Lifecycle Manager 2007 (ILM 2007)
* Microsoft Identity Integration Server (MIIS) 2003
* Zero Touch Provisioning (ZTP)

### Microsoft Identity Lifecycle Manager 2007

[Microsoft Identity Lifecycle Manager 2007 (ILM 2007)](http://www.microsoft.com/windowsserver2003/technologies/idm/ilm.mspx) is the recommended technology for automating user account provisioning. ILM 2007 provides an integrated and comprehensive solution for managing the entire life cycle of user identities and their associated credentials. ILM 2007 builds on the metadirectory and user provisioning capabilities in Microsoft Identity Integration Server 2003 (MIIS 2003) and adds new capabilities for managing strong credentials such as smartcards with Certificate Lifecycle Manager 2007 (CLM 2007). It provides identity synchronization, certificate and password management, and user provisioning in a single solution that works across Microsoft Windows® and other organizational systems. As a result, organizations can define and automate the processes used to manage identities from creation to retirement. Technical resource guidance for ILM 2007 continues to develop, see the [Build a Single-Step Provisioning Workflow featured in the May 2007 edition of TechNet Magazine](http://www.microsoft.com/technet/technetmag/issues/2007/05/Workflow/default.aspx) for additional details.

### Microsoft Identity Integration Server 2003

[Microsoft Identity Integration Server (MIIS) 2003](http://www.microsoft.com/windowsserversystem/miis2003/evaluation/overview/default.mspx) is a centralized service that stores and integrates identity information for organizations with multiple directories. The goal of MIIS 2003 is to provide organizations with a unified view of all known identity information about users, applications, and network resources. Microsoft TechNet provides several resources for planning and implementing automated user provisioning services using MIIS 2003, most notably [Provisioning and Workflow in the Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/p2prov_6.mspx).

### Zero Touch Provisioning

[Zero Touch Provisioning](http://www.microsoft.com/technet/desktopdeployment/bdd/enterprise/ZTPDFTGuide_1.mspx) is the implementation of actions, workflows, and operations required to enable users to self-subscribe to services and software. ZTP requires that identities are already being managed, and it extends provisioning from identity and access services to other IT service requests in the organization. ZTP allows organizations to move to a managed, self-service provisioning portal that allows delegates to perform such common provisioning tasks as password resets, e-mail provisioning, and elective application installation. ZTP is based on Microsoft BizTalk Server and requires the use of Systems Management Server 2003. ZTP provides a base to reliably provision enterprise or hosted commercial services and applications, resulting in reduced administrator intervention during the provisioning phase. An initial version of ZTP using BizTalk Server 2004 is available via the [Solution Accelerator for Business Desktop Deployment Enterprise Edition Version 2.5](http://www.microsoft.com/downloads/details.aspx?FamilyID=16dc014b-39d1-49ee-ac6a-e3077e4e2607) download. For more recent versions of Zero Touch Provisioning using BizTalk Server 2006, contact [Microsoft Services](http://www.microsoft.com/services/microsoftservices/default.mspx).

### Evaluating the Technologies

Each of the technologies listed above, as well as technologies available from other providers, can help you achieve automated account or identity object provisioning. Additionally, ZTP solutions add another layer of functionality to identity life-cycle management by providing automated provisioning of common service requests, such as self-service requesting and provisioning of new applications and password resets. We recommend reading the highlighted resources when evaluating your technology options, along with associated costs and implementation requirements.

### Planning the Solution

You can design and plan a provisioning solution in the same way that you would design and plan any other IT project. The process requires gathering requirements; implementing conceptual, logical, and physical designs; building a proof of concept; and then creating project plans, a schedule, and a budget. For more information, see [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx?mfr=true).

For more information about architecting a MIIS 2003 solution, see the [MIIS 2003 Design and Planning Collection](http://go.microsoft.com/fwlink/?LinkId=50489).

Project-specific guidance for ILM 2007 is currently under development. The guidance highlighted in the [Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx) is built for and tested against MIIS 2003, but most of the core concepts can be applied to equivalent functionality as well as planning and deployment objectives for ILM 2007. Visit the [technical library for ILM 2007](http://technet2.microsoft.com/ILM/en/library/a4d5346d-418c-497c-bbab-ff49e94e982b1033.mspx?mfr=true) for additional guidance.

## Phase 4: Deploy

Once your provisioning solutions have been evaluated and projects are planned, the final phase is Deployment. There are several prerequisites to deploying a workflow and provisioning solution, and this section focuses only on the prerequisites of identity and access related to provisioning:

* [Identity Aggregation and Synchronization](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P2Ident.mspx?mfr=true) in place.
* [Data Access Application Block for .NET 2.0](http://go.microsoft.com/fwlink/?linkId=67589) is installed.
* [Microsoft Message Queuing (MSMQ) component](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true) is installed.

Once prerequisites are met, implementation consists of configuring MIIS 2003 or ILM 2007 and beginning to perform identity management operations, including importing and synchronizing all existing data so that you are ready to conduct ongoing operations.

For more information on deploying a provisioning solution using ILM 2007, see [Build a Single-Step Provisioning Workflow](http://www.microsoft.com/technet/technetmag/issues/2007/05/Workflow/default.aspx) featured in the May 2007 edition of TechNet Magazine.

For more information about implementing MIIS 2003 for user account provisioning, see [Implementing the Solution in the Workflow and Provisioning section of the Microsoft Identity and Access Management Series](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/default.mspx?mfr=true).

## Further Information

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

To see how Microsoft handles provisioning, go to <https://www.microsoft.com/technet/itshowcase/content/ensidcon.mspx>.

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Defined current identity object provisioning workflows in your organization, as well as areas to improve or optimize. |
|  | Identified technologies used to manage object identity life cycles. |
|  | Implemented a consolidated solution to automate common user account provisioning workflows. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for Centralized and Automated User Provisioning capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for user provisioning to ensure that user access and network security levels are maintained to a known standard.

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

# Requirement: Directory-based Authentication of External Customers and Business Partners

## Audience

You should read this section if you do not use a directory-based tool to enable authenticated access to external customers and business partners.

## Overview

In the *Infrastructure Optimization Planning Guide for Implementers: Basic to Standardized* guide, we discussed using directory services for user authentication. To move to the Dynamic level, Core Infrastructure Optimization requires the ability to securely extend authentication to external customers and business partners when needed. Most organizations will need to provide information to external customers and business partners in some form on an ongoing basis. IT organizations can use identity federations to make decisions based on identity data from other organizations, while also sharing selected information about their own users' identities. A federation represents an agreement between two organizations with a common goal and is usually structured so that each organization retains the management of its own internal information, access policies, and identity objects.

## Phase 1: Assess

Data and information is inevitably shared to external stakeholders for your organization. During the Assess phase, you will take an inventory of the shared data and how that is currently performed. The results of the Assess phase will be documentation listing resources where data and information is commonly shared and showing where a federation can improve efficiency by providing access to trusted external stakeholders.

## Phase 2: Identify

Depending on the resources identified during the Assess phase, you may determine that some of the existing workflows can be made more secure by using manual processes to control the flow of data. In cases where the secured and authenticated access by external customers or partners does not compromise the organization, you will use the Identify phase to isolate priority resources, partners, and customers to participate in identity federation solutions. The results of the Identify phase will include a detailed list of those organizations, along with related resources and a corresponding list of identity objects targeted for the initial project.

## Phase 3: Evaluate and Plan

As a result of progressing through the Core Infrastructure Optimization Model and achieving the prerequisites of the Standardized level, your organization will have at minimum an Active Directory infrastructure in place. We also assume in the model that organizations at the Rationalized level have knowledge of Active Directory Application Mode (ADAM). During the Evaluate and Plan phase, you will examine the technologies that can extend directory service authentication to external stakeholders, primarily Active Directory Federation Services (ADFS), and plan for the solution implementation. For additional options to manage access to extranet resources, see [Extranet Access Management: Approaches to Extranet Access Management](http://www.microsoft.com/technet/security/guidance/identitymanagement/idmanage/P3Extran_1.mspx?mfr=true) on Microsoft TechNet.

### Active Directory Application Mode (ADAM)

[ADAM](http://technet2.microsoft.com/windowsserver/en/library/86bd57d5-37e7-4212-a28e-39ffb1215c8a1033.mspx) provides directory services specifically for directory-enabled applications. ADAM does not require or rely on Active Directory domains or forests. However, in environments where Active Directory exists, ADAM can use Active Directory for the authentication of Windows security principals.

### Active Directory Federation Services (ADFS)

[Active Directory Federation Services (ADFS)](http://technet2.microsoft.com/WindowsServer/f/?en/library/1f6e9e6e-c179-4dd2-bd1d-c74dd4ebf56b1033.mspx) is a component in [Microsoft Windows Server 2003 R2](http://www.microsoft.com/windowsserver2003/default.mspx) that provides browser-based clients (internal or external to your network) with single sign-on (SSO) access to protected Internet-facing applications, even when the user accounts and applications are located in completely different networks or organizations.

When an application is in one network and a user account is in another network, typically the user is prompted for secondary credentials when he or she attempts to access the application. These secondary credentials represent the user's identity in the realm where the application resides and are usually required by the Web server that hosts the application so that it can make the most appropriate authorization decision.

With ADFS, organizations can bypass requests for secondary credentials by providing trust relationships (federation trusts) that they can use to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities, but each organization can also securely project and accept identities from other organizations.

ADFS is tightly integrated with Active Directory. ADFS retrieves user attributes from Active Directory, and it authenticates users against Active Directory. ADFS also uses Windows Integrated Authentication.

By employing ADFS, you can extend your existing Active Directory infrastructures to provide access to resources that are offered by trusted partners across the Internet. These trusted partners can include external third parties or other departments or subsidiaries in your organization.

#### Federation Scenarios

ADFS supports three federated identity scenarios:

* Federated Web SSO
* Federated Web SSO with forest trust
* Web SSO

Federated Web SSO and Web SSO are the scenarios required to move to the Dynamic level in the Core Infrastructure Optimization Model.

##### Federated Web SSO

The ADFS Federated Web SSO scenario involves secure communication that often spans multiple firewalls, perimeter networks, and name resolution servers, in addition to the entire Internet routing infrastructure. Communication over a federated Web SSO environment can help foster more efficient and secure online transactions between organizations that are joined by federation trust relationships.

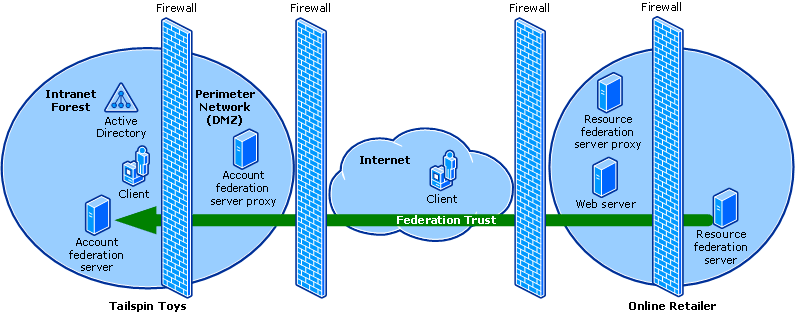


Figure 3. Federated Web SSO

##### Federated Web SSO with Forest Trust

The ADFS Federated Web SSO with Forest Trust scenario involves two Active Directory forests in a single organization, as shown in the following illustration.

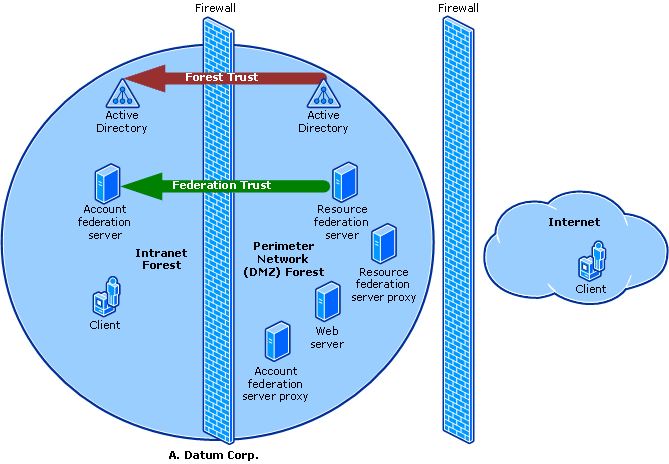


Figure 4. Federated Web SSO with Forest Trust

##### Web SSO

In the ADFS Web SSO scenario, users must authenticate only once to access multiple Web-based applications. In this scenario, all users are external, and no federation trust exists. Because the Web servers must be Internet-accessible and also be joined to the Active Directory domain, they are connected to two networks; that is, they are multihomed. The first network is Internet facing (the perimeter network) to provide the needed connectivity. The second network contains the Active Directory forest (the protected network), which is not directly Internet accessible.

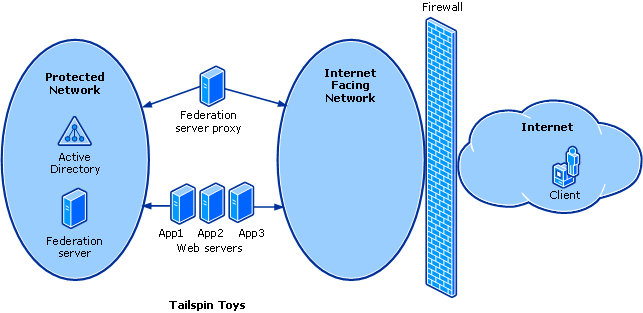


Figure 5. Web SSO

### Planning for ADFS Implementation

When planning for an ADFS implementation, you will need to consider technology prerequisites, project goals, partner or federation planning, federated application strategy, and infrastructure design.

#### Prerequisites

You will need to have the following services or functionalities in place prior to implementing ADFS:

* **Active Directory.** An Active Directory domain is required only for the resource federation server. It is not used to host customer accounts.
* **ADAM.** ADAM is used to contain the customer accounts that will be used to generate ADFS tokens. For more information about Active Directory or ADAM, see [Appendix B: Reviewing Key ADFS Concepts](http://technet2.microsoft.com/WindowsServer/en/library/74513c82-68de-465e-aead-b4eef9a221cb1033.mspx).
* **Account/resource federation server.** This federation server serves in both the account role and the resource role. The account/resource federation server is configured so that the Federation Service includes values for both an application and an account store—in this case, ADAM—that contains the customer accounts. For more information, see [Review the role of the federation server in the account partner organization](http://technet2.microsoft.com/WindowsServer/en/library/d3df643a-e205-475b-b4b4-898dbf67fb4e1033.mspx) and [Review the role of the federation server in the resource partner organization](http://technet2.microsoft.com/WindowsServer/en/library/e27e9107-8f2a-48e8-a35e-5722ce4d347e1033.mspx).
* **ADFS-enabled Web server.** The ADFS-enabled Web server can host a claims-aware application or a Windows NT® token–based application. The ADFS Web Agent confirms that it receives valid ADFS tokens from customer accounts before it allows access to the protected Web site. For more information, see [When to create an ADFS-enabled Web server](http://technet2.microsoft.com/WindowsServer/en/library/c9383874-1da8-4670-bb1f-30e8439016881033.mspx).
* **Customer.** While on the Internet, the customer accesses an ADFS-secured Web application through a supported Web browser. The customer client computer on the Internet communicates directly with the federation server for authentication.

#### Primary Planning Considerations

The following guides are technical resources for planning ADFS services. Use these resources to help develop a project plan to implement ADFS services.

* [Understanding the ADFS Design Process](http://technet2.microsoft.com/WindowsServer/en/library/ffc787f4-74ad-4efc-bc4c-0cd505e7c6e61033.mspx)
* [Identifying Your ADFS Deployment Goals](http://technet2.microsoft.com/WindowsServer/en/library/8657d568-e8a6-4e89-b76a-cdde7c1ba18e1033.mspx)
* [Mapping Your Deployment Goals to an ADFS Design](http://technet2.microsoft.com/WindowsServer/en/library/332933a0-cd7f-4cad-b557-4b580f32d0ba1033.mspx)
* [Evaluating ADFS Design Examples](http://technet2.microsoft.com/WindowsServer/en/library/4592047c-cf5a-48e6-ba87-e07a31d2de351033.mspx)
* [Planning Partner Organization Deployments](http://technet2.microsoft.com/WindowsServer/en/library/1921c616-5581-4c3f-8032-61a7773373631033.mspx)
* [Designing a Federated Application Strategy](http://technet2.microsoft.com/WindowsServer/en/library/3600eeb2-758b-4d0a-acb7-de902e7c56961033.mspx)
* [Planning ADFS-Enabled Web Server Placement](http://technet2.microsoft.com/WindowsServer/en/library/422c5b42-4f43-4e7d-8380-52226173d82e1033.mspx)
* [Planning Federation Server Placement](http://technet2.microsoft.com/WindowsServer/en/library/84e293d6-e91a-4705-a348-6ed353ee3d221033.mspx)
* [Planning Federation Server Proxy Placement](http://technet2.microsoft.com/WindowsServer/en/library/295f6e6e-bd4c-4d0a-8058-538456e8077e1033.mspx)
* [Planning for ADFS Capacity](http://technet2.microsoft.com/WindowsServer/en/library/2b549697-ece0-40e5-ad3e-7d15d6b9087d1033.mspx)
* [Finding Additional ADFS Resources](http://technet2.microsoft.com/WindowsServer/en/library/771b500e-f6a0-4e85-b1cd-61934056c3e81033.mspx)
* [Appendix A: Reviewing ADFS Requirements](http://technet2.microsoft.com/WindowsServer/en/library/5f0775d0-4b86-4482-a76a-552d7351f0ab1033.mspx)
* [Appendix B: Reviewing Key ADFS Concepts](http://technet2.microsoft.com/WindowsServer/en/library/74513c82-68de-465e-aead-b4eef9a221cb1033.mspx)
* [Appendix C: Documenting Your ADFS Design](http://technet2.microsoft.com/WindowsServer/en/library/e86018b1-e25d-4335-ad75-afb64b5144f51033.mspx)

## Phase 4: Deploy

After you collect information about your environment and decide on an Active Directory Federation Services (ADFS) design by following the guidance in the [ADFS Design Guide](http://technet2.microsoft.com/WindowsServer/en/library/1f6e9e6e-c179-4dd2-bd1d-c74dd4ebf56b1033.mspx), you can begin to plan the deployment of your organization's ADFS design. With the completed ADFS design and the information in this topic, you can determine which tasks to perform to deploy ADFS in your organization. For detailed technical guidance to deploy ADFS, see the Windows Server 2003 R2 technical library’s [ADFS Deployment Guide](http://technet2.microsoft.com/windowsserver/en/library/73bf15f4-e10c-48e3-9ff8-6da5ff2cde211033.mspx).

For a step-by-step guide to setting up and administering ADFS, go to <http://technet2.microsoft.com/WindowsServer/f/?en/library/d022ac37-9b74-4ba1-95aa-55868c0ebd8c1033.mspx>.

## Further Information

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

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Validated need and uses for providing authenticated access to external entities. |
|  | Determined strategies and policies for providing external access to defined resources. |
|  | Implemented technologies to ensure secure access for defined external users to defined services. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for Directory-based Authentication of External Customers and Business Partners capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for partner and client authentication.

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

Capability: Desktop, Device and Server Management

# Introduction

Desktop, Device and Server Management is the second Core Infrastructure Optimization capability.

The following table describes the high-level challenges, applicable solutions, and benefits of moving to the Dynamic level in Desktop, Device and Server Management.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Users rely on help desk for various provisioning needs, resulting in higher operating costs  Sprawling servers and applications demand more resources and increase costs for electricity, real estate, and staff  User mobility lags due to a lack of automated solutions for deploying and updating ultra-mobile PC software  **IT Challenges**  Lack of end-to-end capacity planning results in reduced application availability, performance, and capacity challenges  IT Application teams slowly deliver and roll out updates and new applications due to configuration conflicts with IT operations and users | **Projects**  Implement automated infrastructure capacity planning  Implement a comprehensive solution for mobile device management  Implement virtual technology solution for testing and consolidation | **Business Benefits**  Remote API functions for accessing files and databases located on devices  Agile IT infrastructure helps business respond well to competitive threats  **IT Benefits**  Single management server infrastructure for servers, desktops, and devices  Reduced development time and costs with familiar development tools that enable corporate developers to utilize existing code, skills, and assets  Consistent profiles across systems enhance various device-management functions  Centralized solution for installing software and sharing content with mobile devices  Highly automated IT services reduce costs and improve consistency |

The Dynamic level in the Infrastructure Optimization Model addresses the more advanced areas of mobile device and service management including the following requirements:

* Automated Infrastructure Capacity Planning for Primary IT Services
* Management of Mobile Devices
* Virtualization to Dynamically Move Workloads from Server to Server

# Requirement: Automated Infrastructure Capacity Planning for Primary IT Services

## Audience

You should read this section if you do not have automation implemented for infrastructure capacity planning for your primary IT services.

## Overview

In the *Infrastructure Optimization Planning Guide for Implementers: Basic to Standardized* guide, you read about monitoring the availability of critical servers. To move to the Dynamic level, you need to analyze the capacity of your enterprise servers, such as e-mail, and create a plan to optimize current and future needs.

Capacity planning is part of [capacity management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcapmg.mspx), which is the process of planning, analyzing, sizing, and optimizing capacity to satisfy demand in a timely manner and at a reasonable cost. This process should be proactive and responsive to business needs because the business cannot add resources after a capacity problem has happened without affecting performance.

Capacity management focuses on procedures and systems, including specification, implementation, monitoring, analysis, and tuning of IT resources and their resulting service performance. Capacity requirements are based on qualitative and quantitative standards set by the service level management process and specified within the provisions of a service level agreement (SLA) or operating level agreement (OLA). The capacity management process relies on a set of iterative tasks—monitoring, analysis, modeling, optimizing, and change initiation—to achieve its goals.

## Phase 1: Assess

The Assess phase and capacity planning begins with identifying which services are primary to your organization and ranking those services by priority. For many organizations, these systems will include those services necessary to operate the business, such as Enterprise Resource Planning (ERP) systems, and those necessary to facilitate communication, such as messaging services. The results of this phase should be a prioritized list of the primary services in your organization, along with the IT or network infrastructure resources required to operate these services.

## Phase 2: Identify

The Identify phase is responsible for nominating which services identified during the Assess phase will be candidates for automated capacity planning. Considerations will include whether your organization has control of the elements in that service that dictate capacity constraints. Hosted services delivered by a vendor, for example, will be subject to service level agreements between your organization and the vendor; in this case, the vendor is typically responsible for capacity planning. The results of the Identify phase will be a manifest of those services.

## Phase 3: Evaluate and Plan

During the Evaluate and Plan phase, you will examine the processes associated with developing automated capacity planning or modeling solutions, as well as the technologies that can be used to automate these processes. It is likely that prepackaged software in most cases will not provide the breadth of information and service coverage necessary for your organization.

### Capacity Management Process Flow

[Capacity management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfcapmg.mspx) is an iterative process with several activities being performed throughout the process. In order to keep this document brief, only a selection of the core capacity management tasks (see Figure 6) has been chosen for a detailed explanation.

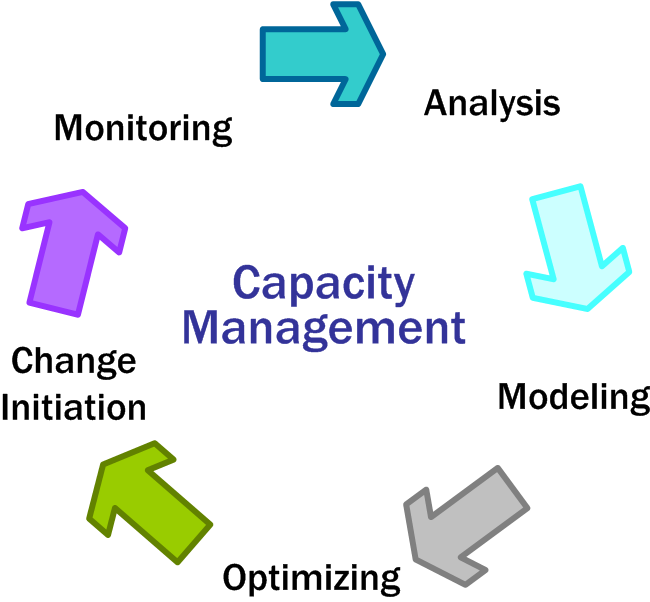


Figure 6. Capacity management as an iterative process

#### Monitoring

Capacity management involves the internal operating level requirements and associated metrics for each of the key IT layers that contribute to the overall SLA. It is important that the utilization of each resource and service be monitored on an ongoing basis to ensure that hardware and software resources are being used optimally and that all agreed-upon service levels can be achieved.

#### Analysis

In the Analysis phase, the data monitored and collected is analyzed and used to carry out tuning exercises and establish profiles. These profiles are important since they allow the proper identification and adjustment of thresholds and alarms. When exception reports or alarms are raised, they need to be analyzed and reported upon, and corrective action needs to be taken.

#### Modeling

Modeling is a central element of the capacity management process. Modeling techniques and effective use of simulation software make it possible to investigate capacity planning “what-if” scenarios in order to build a model that simulates the desired outcome.

Modeling is the activity required by the Infrastructure Optimization Model at the Dynamic level; it requires that data collected from monitoring and analysis is in place to create automated capacity planning tools, whether developed by your organization or as part of a packaged software offering. Although the modeling element is the minimum requirement of the Dynamic level, it is recommended that the solutions used to automate capacity planning be accurate enough to use for new implementation or optimization of the identified primary services.

#### Optimizing

Analysis of the monitored data may identify areas of the configuration that could be tuned to better use system resources or improve the performance of the particular service.

#### Change Initiation

Change initiation introduces to the service in production any changes that have been identified by the analysis and tuning activities. This activity includes the identification of the necessary change and subsequent generation and approval of a change request. In some cases, implementation of the change runs concurrent to the service; in other cases, the type of change may require the service to be temporarily stopped.

### Monitoring Technologies

The main tools from Microsoft that assist you in gathering server performance and network performance data are Windows System Monitor and Network Monitor, respectively. System Monitor is the recommended resource that is used for creating a server sizing model. Use System Monitor to identify standards for acceptable server performance and to recognize periods of peak performance. The data that is collected is instrumental in both establishing and maintaining SLAs.

[Network Monitor 2.1](http://technet2.microsoft.com/WindowsServer/en/library/ad2b59d1-0fb8-45e3-9055-a5aeba8817a91033.mspx?mfr=true), included with [Microsoft Systems Management Server 2003](http://www.microsoft.com/technet/sms/sms2003_default.mspx) (SMS), makes it easier to monitor and analyze network traffic that is generated among computers on the network. You use Network Monitor to identify heavily used subnets, routers, and WAN connections, to recognize where network bottlenecks occur, and to develop trends to optimize network infrastructure and server placement or expansion.

For more information about using SMS 2003 for capacity planning and analysis, go to <http://www.microsoft.com/technet/sms/2003/library/spgsms03/spsms13.mspx>.

### Capacity Planning Technologies

[Microsoft System Center Capacity Planner 2006](http://www.microsoft.com/systemcenter/sccp/overview/default.mspx) helps size and plan deployments of Microsoft Exchange Server 2003 and Microsoft Operations Manager (MOM) 2005 by providing you with the tools and guidance to deploy efficiently while planning for the future by allowing for "what-if" analyses in the following ways:

* Plan the correct amount of infrastructure needed for a new application to meet service level goals.
* Infrastructure planning and optimization.
* Proactive performance planning.
* Performance analysis and predictive reporting.

System Center Capacity Planner 2006 is designed to create a system architecture model for deploying Exchange Server 2003 or MOM 2005. A typical system architecture model consists of the following information:

* **Topology.** Site locations, types of networks, network components, and network characteristics (bandwidth, latency)
* **Hardware.** Server distribution and characteristics, server and network mapping
* **Software.** Server role and service mapping, file and storage device mapping
* **Usage profiles.** Site usage and client usage

After creating a model, a simulation provides a summary and details about the performance of the application and its supporting components.

### Custom Tools

Automated capacity planning tools can vary in type and level of functionality. It is very common to feed monitoring and analysis data into a spreadsheet and develop formulas to determine capacity based on changes to defined fields in the spreadsheet. At the other end of the spectrum are tools incorporating an even greater level of knowledge and detailed graphical modeling of topologies, such as the System Center Capacity Planner. Whether your solution is developed in-house or by a third party, the primary requirement of the Evaluate and Plan phase is to ensure that the tools or methods used to automate capacity planning are accurate and trusted for planning and optimizing the infrastructures that affect your organization’s primary IT services.

## Phase 4: Deploy

The Deploy phase of an automated capacity planning project ensures that the tools selected are a key part of the planning process and maintained on an ongoing basis for new implementations and optimization projects involving your organization’s primary IT services. Models should be updated as new factors or technologies are introduced into your environment, such as the use of server clustering, blade servers, or virtualization. A deployment of these tools can only be successful if agreements are in place to standardize on their recommendations and provide sustained engineering or updates as necessary.

## Further Information

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

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Identified primary IT service candidates for automated capacity planning. |
|  | Created capacity models to automate capacity planning or implemented capacity planning tools. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level relating to automated infrastructure capacity planning for primary IT services capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for analyzing critical services.

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

# Requirement: Management of Mobile Devices

## Audience

You should read this section if you do not have a defined life-cycle management strategy for your mobile devices.

## Overview

In the *Infrastructure Optimization Planning Guide for Implementers: Basic to Standardized* and *Infrastructure Optimization Planning Guide for Implementers: Standardized to Rationalized* guides, you read about several topics associated with mobile device management as well as topics associated with desktop computer management. To move to the Dynamic level, you need to apply many of the same principles and capabilities from your desktop management activities to your mobile devices and therefore extend your current mobile device management capabilities.

The integration of mobile devices, the Internet, and wireless connectivity provides an exciting opportunity for organizations to extend the reach of their information and services to mobile professionals. Current mobile devices are quickly approaching the computational and functional levels generally associated with portable computers. The advantages and disadvantages of these devices are also similar to portable computers and while there is a definite opportunity to improve productivity, there is an equivalent threat of data loss or security breach.

As the use of mobile devices increases in your organization, the need to control the types of mobile devices also increases. Without standardization, the mix of mobile devices connecting to your corporate network would be nearly impossible to manage. User authentication, standardization of operating systems, patch management, and other everyday administrative controls can only be effectively managed when you have established a company standard for each type of mobile device.

The Core Infrastructure Optimization Model profiling or question set separates the areas covered in this requirement into several individual requirements. The focus of these questions is to ensure that many of the capabilities exercised for portable computers are eventually matched by the management capabilities for mobile devices. In many cases, the tools to perform tasks for desktop deployment or management do not have equivalents for mobile devices; however, the concepts are for the most part the same.

For guidance in planning a mobile device solution, go to <http://www.microsoft.com/technet/archive/itsolutions/mobile/deploy/mblwirel.mspx?mfr=true>.

For more information on managing mobile devices, go to <http://www.microsoft.com/technet/solutionaccelerators/mobile/evaluate/mblmange.mspx>.

## Phase 1: Assess

As a requirement of the Standardized and Rationalized levels, your organization should already be maintaining a detailed inventory of mobile devices connecting to your organization’s resources. The Assess phase requires that this inventory be updated and available for subsequent phases.

## Phase 2: Identify

The Identify phase examines the capabilities needed to fulfill the requirements of the Dynamic level. The requirements of the Dynamic level include the following:

* Access to LOB applications
* Defined basic images
* Automated update of configurations and applications
* Quarantine solution
* Automated patch management
* Automated asset management

By achieving the Rationalized level, your organization should already have mechanisms in place to access Web-based LOB applications, automate software and configuration files distribution, automate patch management, and automate asset management. The net new capabilities for the Dynamic level then are defining and maintaining basic mobile device images and establishing a quarantine solution for mobile devices.

## Phase 3: Evaluate and Plan

The goal of the Evaluate and Plan phase is to identify the technologies needed to manage mobile device images and establish an effective quarantine mechanism to detect whether mobile devices comply with organizational standards and to quarantine them from resources when they are determined to be noncompliant.

This section of the guide addresses the following areas of mobile device management:

* Defined basic images for mobile devices
* Quarantine solution

### Defined Basic Images for Mobile Devices

Defining standard images for mobile devices ensures that their configuration is known and manageable across the organization and generally consists of three primary activities:

* Device standardization
* Image standardization
* File distribution

Until the technologies are common for organizations to install or refresh images on mobile devices, image standardization will be the responsibility of the device manufacturers or service providers.

#### Device Standardization

Members of your mobile workforce can carry many different types of mobile devices. It would be very inefficient to maintain a standard set of images for each type of cell phone or PDA that your users might choose to use. Choosing a company standard for each type of mobile device is the only way to efficiently and securely manage these devices. Once a device has been specified, a standard operating system and set of core applications can be chosen and maintained.

#### Image Standardization

Mobile device image management is much different than imaging desktop or server devices. A typical scenario will involve the organization standardizing on a device type and mobile operating system. The devices and mobile operating systems are then built and delivered by the device manufacturer or service provider; this is often attributed to the reduced asset life cycle of mobile devices in the organization and the lack of technology and interfaces available to install operating systems as you would on a network-connected or media-bootable client or server. In this case, image standardization consists of determining and enforcing a policy for standard mobile device operating systems and ensuring that required configurations and applications are applied to mobile devices. You can use the device provisioning tools that are available in the Windows Mobile® Software Development Kits (SDKs) to configure settings on the devices; to add, update, and remove software from the mobile devices; or to change the functionality of the mobile devices. For more information, see the [Step-by-Step Guide to Deploying Windows Mobile-based Devices with Microsoft Exchange Server 2003 SP2: Step 8 - Manage and Configure Mobile Devices](http://www.microsoft.com/technet/solutionaccelerators/mobile/deploy/msfp_8.mspx).

#### File Distribution

Since mobile devices tend to come with the operating system installed, you will need to have a mechanism for installing the standard applications and configuration files that each mobile device is required to have. There are several tools available for software distribution to mobile devices, such as:

* [Device Management Feature Pack](https://www.microsoft.com/technet/downloads/sms/2003/featurepacks/dmfp.mspx) for [Microsoft Systems Management Server 2003](https://www.microsoft.com/technet/sms/sms2003_default.mspx)
* [Afaria Software Manager](http://www.ianywhere.com/datasheets/afaria_software_manager.html) from [iAnywhere](http://www.ianywhere.com/)

These tools give you the ability to distribute a standardized set of applications to your mobile devices.

### Quarantine Solution for Mobile Devices

Even with the best plans and policies in place to ensure that mobile devices comply with all security requirements of your organization, there will be times when these measures will be deactivated, circumvented, or breached. When a mobile device has been infected by malicious software or has had its security policies compromised, and it then connects to your network, your network and all assets and data on the network are compromised. You need a method to ensure that mobile devices connecting to your network comply with all of your corporate security policies.

In the [Quarantine Solution for Unpatched or Infected Computers requirement](#_Quarantine_Solution_For_1) later in this document, we discuss using virtual private networks (VPN) and quarantine controls on client computers to restrict network access to computers not meeting minimum configuration compliance requirements. Microsoft partner solutions—such as [Bluefire Mobile Security VPN](http://www.bluefiresecurity.com/products/vpn/)—can enable quarantine protection for mobile devices and offer many of the same advantages of quarantine used with client computers.

## Device Management Products

The Microsoft [Systems Management Server (SMS) 2003 Device Management Feature Pack](http://www.microsoft.com/technet/downloads/sms/2003/featurepacks/dmfp.mspx) offers a comprehensive device management solution for mobile devices [Windows CE](http://msdn.microsoft.com/embedded/windowsce/default.aspx) (3.0 or later) and [Windows Mobile](http://www.microsoft.com/windowsmobile/articles/benefits.mspx) software for Pocket PCs (2002 or later) with updated support for Windows Mobile 5.0 and Windows Mobile Pocket PC Phone Edition 5.0.

### Partner Solutions

The following summary material was provided by each vendor. Microsoft does not endorse or recommend particular solutions. The solutions listed below can help your organization achieve near parity between mobile device and desktop management:

* **B2M** ([www.b2m-solutions.com](http://www.b2m-solutions.com)). Offers the mprodigy product line designed for blue collar and industrial markets.
* **BeCrypt** ([www.becrypt.com](http://www.becrypt.com)). Specializes in producing security products for laptops, Tablet PCs, and desktops, as well as for Pocket PC/Windows Mobile 5 PDA devices.
* **Bluefire Mobile Security Suite** ([www.bluefiresecurity.com](http://www.bluefiresecurity.com)). A comprehensive suite of products that work together to help secure mobile devices.
* **iAnywhere** ([www.ianywhere.com](http://www.ianywhere.com/)). A subsidiary of Sybase. Their Afaria management suite provides comprehensive management capabilities.
* **Odyssey’s Athena** product ([www.odysseysoftware.com](http://www.odysseysoftware.com)). A device management solution that provides comprehensive management for Windows Mobile®, Windows CE, Win32®, and Windows XP embedded devices.
* **Perlego Mobile Device Lifecycle Management (MDLM)** (<http://www.perlego.comwww.perlego.com>). This suite provides remote control, data assurance, and content distribution tools to protect and manage devices and their data.

## Further Information

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

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Standardized devices and device images from manufacturers or service providers. |
|  | Defined configuration compliance standards enforced on all mobile devices prior to connecting to data resources. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for Management of Mobile Devices in the Infrastructure Optimization Model.

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

# Requirement: Virtualization to Dynamically Move Workloads from Server to Server

## Overview

In the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide, we discussed the requirement for developing a plan for consolidation using virtualization. The requirement at the Rationalized level was limited to planning and testing virtualization technologies. At the Dynamic level, the requirement for virtualization extends to implementation of production applications or services. This requirement continues to call out the virtualization best practices highlighted in the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx). Additional guidance for using virtualization in the context for development and test can be found in the [Windows Server System Reference Architecture Virtual Environments for Development and Test](http://www.microsoft.com/technet/solutionaccelerators/wssra/ve/default.mspx) guide.

Consolidation of physical infrastructure, in general, is an effective business strategy and can be an effective tool in maintaining hardware utilization. Additionally, the nature of virtualization allows you to assign system resources to production virtual machines as necessary; this is different from a 1:1 server application physical environment, where only hardware upgrades or downgrades can be used to adjust performance.

## Phase 1: Assess

At the Rationalized level and as discussed in the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide, you were required to take an inventory of applications and infrastructure in your organization.

## Phase 2: Identify

At the Rationalized level and as discussed in the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide, you were required to nominate the appropriate services targeted for virtualization in your organization.

## Phase 3: Evaluate and Plan

At the Rationalized level and as discussed in the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide, you were required to evaluate virtualization technologies and plan for virtualization deployment in your organization.

## Phase 4: Deploy

The Deploy phase is responsible for implementing a tested virtualization strategy selected at the Rationalized level. This phase includes establishing the consolidated virtual machine environment and virtualizing applications in the consolidated environment. The following figure from the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx) illustrates how planning and design tasks fit in the overall scope and sequence of the consolidation, migration, and virtualization of LOB applications using Microsoft Virtual Server 2005. For detailed information, see the [Implementation Guide in the Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaimg.mspx).

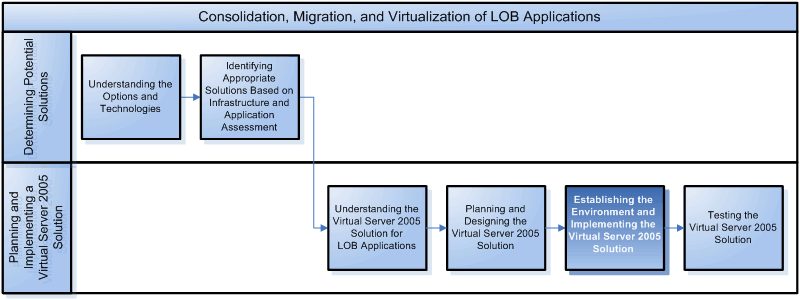


Figure 7. LOB application virtualization process

Implementation of a virtual server solution starts with establishing a consolidated environment, including both building and stabilizing the environment. This includes:

* Preparing the infrastructure.
* Setting up hardware and software platforms for the destination servers.
* Deploying the tools required to migrate and virtualize the source servers.

### Setting Up the Infrastructure

The first step in building the consolidated environment is to set up the infrastructure, ensuring that the required network connectivity and infrastructure services (including directory services, Domain Name System (DNS), and Windows Internet Name Service (WINS) are in place. In addition, appropriate accounts and groups, and a migration account, should be created as appropriate to the deployment requirements.

### Setting Up Tools

[Virtual Server 2005 Migration Toolkit (VSMT)](http://www.microsoft.com/technet/virtualserver/downloads/vsmt.mspx) requires the availability of at least one Automated Deployment Services (ADS) Controller in the organization. The Controller can schedule jobs to run on devices (computers added to the ADS database) that have the deployment agent running on the system. The deployment agent can run on Windows 2000 Server or Windows Server 2003.

### Stabilizing the Virtual Machine Infrastructure

After the infrastructure for the consolidated environment is designed and built, ensure that the target state meets the goals stated for implementation. The environment should be stabilized before it is put into production.

Before migrating servers to the consolidated environment, ensure that:

* The consolidated environment and supporting infrastructure is operational.
* Required hotfixes and security updates are installed on the host operating system and each guest operating system.
* Event logs of the consolidated and supporting servers are cleared and there are no warnings, errors, or alerts.
* The consolidated environment meets the availability goals.
* The consolidated environment provides the capacity requirements.
* Users, administrators, and LOB applications have proper access to the service resources.
* The consolidated environment provides the required level of I/O performance.
* Migration tools have been implemented.

### Deploying Virtualized Services into Operations

After building and stabilizing the consolidated environment, you should be ready to virtualize services by capturing images of the source servers and creating virtual machines in the new environment. The deployment process for virtualization contains the following steps:

1. **Gather source information**. Collect hardware and software information about the source server to complete pre-deployment validation of the source server.
2. **Load updated system files into the patch cache**. Add required patch files to the VSMT patch cache to ensure that they are available to VSMT for installation after the image is deployed to the virtual machine.
3. **Filtering devices and services**. Identify source server hardware-specific devices and services to disable during virtualization.
4. **Generate the command files and task sequences**. Generate the necessary script files and ADS task sequences.
5. **Capture the image of the physical computer**. Capture the disk partitions of the physical computer.
6. **Deploy the image to a virtual machine**. Create and configure the virtual machine environment and deploy the captured disk partitions.

### Post-Virtualization

After the consolidation and migration of servers is complete and the users are accessing servers in the consolidated environment, consider the following:

* Verify that the migration is complete.
* Create backups of the new environment and retain a baseline of the environment configuration.
* Retire source servers after ensuring that the clients are no longer accessing the servers.
* Complete the documentation of the environment and the project.
* Educate and hand over the operation of the new environment with fully functional service to the corporate IT team.

### Dynamic Movement of Workloads Between Servers

There are two primary options for moving workloads: using Virtual Server 2005 to reallocate system resources from virtual server to virtual server on a single physical host, or moving virtual servers between nodes in a server cluster. The following sections describe both options.

#### Reallocating System Resources in Virtual Server

Virtual Server 2005 provides scripting support through Component Object Model (COM) technology. This enables you to perform additional commands based on a schedule or other event. For example, if you know that a large batch process runs on a SQL Server database once per week, you can use scripts and schedule a task to automatically allocate more memory to the virtual server during the batch process. After the process is completed, another scripted task could reallocate memory back to the state prior to the batch process.

For guidance on using scripts to manage Virtual Server, see [Using Scripts to Manage Virtual Server](http://technet2.microsoft.com/windowsserver/en/library/7944f9f5-5abc-452e-b367-66cc59baa9241033.mspx), or go directly to the [Virtual Server Script Repository](http://www.microsoft.com/technet/scriptcenter/scripts/vs/default.mspx?mfr=true) in the Microsoft Script Center.

#### Virtual Server Host Clustering

[Virtual Server host clustering](http://www.microsoft.com/downloads/details.aspx?familyid=09CC042B-154F-4EBA-A548-89282D6EB1B3&displaylang=en) is a way of combining two technologies—Virtual Server 2005 R2 and the server cluster feature in Windows Server 2003—so that you can consolidate servers onto one physical host server without causing that host server to become a single point of failure. To give an example, suppose you had two physical servers providing client services as follows:

* Microsoft Windows Server 2003, Standard Edition, used as a Web server
* Microsoft Windows NT® Server 4.0 with Service Pack 6a (SP6a), with a specialized application used in your organization

By using host clustering, you can consolidate these servers into one and, at the same time, maintain availability of services if that consolidated server failed or required scheduled maintenance. To do this, you would run each service listed above as a virtual machine on a physical server. You would also configure the server as one node in a server cluster, meaning that a second server would be ready to support the virtual machines in the event of failover. If the first server failed or required scheduled maintenance, the second server would take over support of the services. The result is a dynamic movement of workloads with minimal to no impact on service availability in the event of a failure.

The following figure shows a simple Virtual Server host cluster:

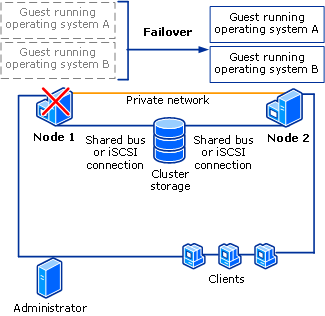


Figure 8. Simple Virtual Server host cluster

It is important to understand that with Virtual Server host clustering, you are clustering the physical hosts, not the applications running on a physical host. Failure of a physical host would cause a second physical host to take over support of a guest, but failure of an application within a guest would not.

## System Center Virtual Machine Manager

[System Center Virtual Machine Manager (SCVMM)](http://www.microsoft.com/systemcenter/scvmm/default.mspx) provides complete support for consolidating multiple physical servers within a virtual infrastructure, thereby helping to increase overall utilization of physical servers. System Center Virtual Machine Manager also enables administrators and authorized users to rapidly provision virtual machines. SCVMM features and benefits include:

* Centralized deployment and management of virtual machines.
* Intelligent placement analysis to determine the best servers for virtualization.
* Quick physical-to-virtual and virtual-to-virtual conversion.
* Ease of use with a familiar interface and seamless integration with other Microsoft products.
* Faster deployments with administrator-managed self-service provisioning.
* Resource efficiency with server consolidation and increased processor utilization.
* Quick automation via PowerShell scripting integration.

For more information on System Center Virtual Machine Manager, visit <http://www.microsoft.com/systemcenter/scvmm/default.mspx>.

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Deployed a subset of production IT services or applications to virtual machines. |
|  | Actively managing and optimizing system resources on shared hardware devices. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for Virtualization to Dynamically Move Workloads from Server to Server capabilities of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for server consolidation and virtualization addressed in the [Solution Accelerator for Consolidating and Migrating LOB Applications](http://www.microsoft.com/technet/solutionaccelerators/ucs/lob/lobsa/lobsaovw.mspx) or download the [Virtual Server Host Clustering Step-by-Step Guide for Virtual Server 2005 R2](http://www.microsoft.com/downloads/details.aspx?familyid=09CC042B-154F-4EBA-A548-89282D6EB1B3&displaylang=en).

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

Capability: Security and Networking

# Introduction

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

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  Enterprise firewall security policies not present for desktops or servers  Enterprise extranet security policies not present  **IT Challenges**  Server event management is reactive, lacking a holistic view of the enterprise  No real-time security event monitoring for desktops or servers | **Projects**  Implement integrated threat management and mitigation solutions across clients and server edge  Deploy model-enabled service level monitoring of desktops, applications, and server infrastructure  Implement quarantine solution for unpatched or infected computers | **Business Benefits**  Achieve proactive security with explicit policies and control from desktop, to firewall, to extranet  Address regulatory compliance thoroughly  Increase user productivity with a stable and secure environment  Respond to security issues quickly and proactively  Mirror business representation through security policy  **IT Benefits**  Thorough monitoring and reporting of server infrastructure, with similar capabilities for desktop  Cost-effective control and visibility over every PC helps IT proactively solve problems before they affect users |

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

* Integrated Threat Management and Mitigation Across Clients and Server Edge
* Model-enabled Service Level Monitoring of Desktops, Applications, and Server Infrastructure
* Quarantine Solution for Unpatched or Infected Computers

# Requirement: Integrated Threat Management and Mitigation Across Clients and Server Edge

## Audience

You should read this section if you do not have integrated threat management and mitigation across clients and server edge.

## Overview

Organizations are facing an onslaught of increasingly targeted and sophisticated attacks on their networks. Protecting network resources and providing seamless access for legitimate activities requires a sophisticated and multifunctional edge gateway solution. To coincide with the Core Infrastructure Optimization Model’s requirement for secure remote access, protection of IT environments from Internet-based threats becomes a necessity.

## Phase 1: Assess

The Assess phase should determine the appropriate server and client edge security needs for your organization and identify which processes are currently in place. Security requirements can vary dramatically from company to company or institution to institution based, for example, on size, industry or field, or regional laws and regulations. Gathering a formal list of risks and requirements of your organization will allow you to evaluate security technologies and how their utilization may affect your organization more effectively.

## Phase 2: Identify

During the Identify phase, you will examine the security and remote access technologies 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. It is recommended that your organization consider server and client edge threat models and corresponding technologies simultaneously when planning for the Dynamic level requirement for a [Quarantine Solution for Unpatched or Infected Computers](#_Quarantine_Solution_for_2).

## Phase 3: Evaluate and Plan

Your organization’s goal during the Evaluate and Plan phase should be to determine a strategy for edge security and to evaluate the technologies available to reduce Internet-based threats. When evaluating your technologies, you should consider security optimization for access to your organization’s file resources and branch offices as well as how your Web and LOB applications are accessed. Your organization can use tools providing enhanced virtual private network (VPN) security and firewalls for Web applications and network resources, as well as tighter access control and enhanced authorization for network resources and LOB applications.

### Internet Security and Acceleration (ISA) Server 2006

[Microsoft Internet Security and Acceleration (ISA) Server 2006](http://www.microsoft.com/technet/isa/default.mspx) is a security gateway that helps protect your applications and resources from Internet-based threats. ISA Server can help your organization to secure access to applications and data. It also helps secure application infrastructure by protecting LOB applications, services, and data across all network layers with stateful packet inspection, application-layer filtering, and comprehensive publishing tools. Using ISA Server, you can streamline your network through a unified firewall and virtual private network (VPN) architecture. ISA Server helps protect your IT environment and reduce security risks and costs, while working to eliminate the effects that malicious software and attackers have on your organization.

### Intelligent Application Gateway (IAG) 2007

[Microsoft Intelligent Application Gateway (IAG) 2007](http://www.microsoft.com/forefront/edgesecurity/iag/overview.mspx) with Application Optimizers provides secure socket layer (SSL) virtual private network (VPN), a Web application firewall, and endpoint security management that enable access control, authorization, and content inspection for a wide variety of LOB applications. Together, these technologies provide mobile and remote workers with easy and flexible secure access from a broad range of devices and locations including kiosks, PCs, and mobile devices. IAG also enables IT administrators to enforce compliance with application and information usage guidelines through a customized remote access policy based on device, user, application, or other business criteria. Key benefits include:

* A unique combination of SSL VPN-based access, integrated application protection, and endpoint security management.
* A powerful, Web-application firewall that helps keep malicious traffic out, and sensitive information in.
* Reduced complexity of managing secure access and protecting business assets with a comprehensive, easy to use platform.
* Interoperability with core Microsoft application infrastructure, third-party enterprise systems, and custom in-house tools.

## Phase 4: Deploy

Evaluated and approved edge security solutions are implemented in the Deploy phase. It is important to perform both usability and fire drill tests for any additional control mechanisms introduced into your environment.

## Further Information

For more information on ISA server products and implementations, go to the ISA Server TechCenter on Microsoft TechNet at <http://www.microsoft.com/technet/isa/default.mspx>.

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Assessed server edge security threats and evaluated threat mitigation solutions. |
|  | Implemented technology solutions to protect against Internet-based threats across the client and server edge. |

# **Requirement: Model-enabled Service Level Monitoring of Desktops, Applications, and Server Infrastructure**

## Audience

You should read this section if you do not have a model-enabled service level monitoring of desktops, applications, and server infrastructure.

## Overview

In the *Core Infrastructure Optimization Implementer Resource Guide: Standardized to Rationalized* guide, we discussed the introduction of best practice [service level management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfslamg.mspx) for several of the requirements at the Rationalized level. Processes introduced for service level management described how services are defined and measured via service level agreements (SLAs). Model-enabled service level monitoring takes these concepts to the Dynamic level by requiring a means to express service models at the system level and report actual service levels—across multiple components—against defined SLAs. Recent advances in technology and industry standards, such as the new Service Modeling Language (SML), allow organizations to implement true model-enabled service monitoring and management.

## Phase 1: Assess

As part of the Rationalized level requirement for ITIL/COBIT-based Process Management, your organization implemented service level management processes and in doing so defined a service catalog. The service catalog lists all of the services currently being provided, summarizes service characteristics, describes the users of the service, and details those responsible for ongoing maintenance. The Assess phase will ensure that the service catalog is complete and up-to-date.

## Phase 2: Identify

The Identify phase will nominate which services within the service catalog are modeled and assign priorities to each service. The list of nominated services will be used in the Evaluate and Plan phase when considering technology options and planning for implementation. This requirement focuses on a subset of IT services, including desktop or client services, application services, and server infrastructure.

## Phase 3: Evaluate and Plan

The goal of the Evaluate and Plan phase is to identify the technologies needed to enable model-enabled service level monitoring of desktops, applications, and server infrastructure. This implies that the selected technology offers both the capability to systematically define services from your organization’s service catalog as well as monitor availability and events from defined services.

### System Center Operations Manager 2007

[Operations Manager 2007](http://technet.microsoft.com/en-us/library/bb381239.aspx) offers a service-oriented monitoring approach that enables you to monitor your end-to-end information technology services, scale monitoring across large environments and organizations, and use Microsoft application and operating system knowledge to resolve operational problems. Operations Manager 2007 is the recommended solution for this requirement in the Core Infrastructure Optimization Model and provides functionality to create and monitor end-to-end service models.

#### Desktop Service Monitoring

Desktop service monitoring in Operations Manager 2007 uses two mechanisms to monitor desktop experience: Agentless Exception Monitoring and Customer Experience Improvement Program data collection.

##### Agentless Exception Monitoring (AEM)

AEM enables you to monitor operating systems for crashes and applications for errors. Error reporting clients are configured with Group Policy to redirect error reports to an Operations Manager 2007 management server, instead of reporting directly to Microsoft. By staging error reports on a management server, Operations Manager 2007 is able to provide detailed views and reports that aggregate error data across your organization. The views and reports provide knowledge about failures and offer solutions, as available, to help resolve the issues.

You can determine how often an operating system or application experiences an error and the number of affected computers and users. This determination enables you to direct your efforts where they will have the greatest benefit to the organization.

When the error reports are anonymously synchronized with Microsoft, per the Privacy Statement for the Microsoft Error Reporting Service, solution responses that are available for the respective errors are provided. You can also use AEM to provide solutions for issues experienced with your internally developed applications.

##### Customer Experience Improvement Program (CEIP)

When you choose to participate in the CEIP, you configure clients with Group Policy to redirect CEIP reports to an Operations Manager 2007 management server, instead of reporting directly to Microsoft. The management servers are configured to forward these reports to Microsoft.

The CEIP reports forwarded from your organization to Microsoft are combined with CEIP reports from other organizations and individual customers to help Microsoft solve problems and improve the Microsoft products and features customers use most often. For more information about the CEIP, see <http://go.microsoft.com/fwlink/?linkid=75040>.

##### Management Packs for Windows-based Workstation Operating Systems and Applications

Following are the Management Packs for Windows-based workstation operating systems and applications that are included with Operations Manager 2007:

* Windows Vista®
* Windows XP
* Windows 2000
* Microsoft Information Worker

#### Distributed Application Service Monitoring

A distributed application service in Operations Manager 2007 monitors the health of a distributed application that you define. It creates the monitors, rules, views, and reports necessary to monitor your distributed application and the individual components that it contains. When creating a distributed application in Operations Manager 2007, you first create the service that defines the distributed application monitoring object at a high level. Then you define the individual components that are part of the distributed application you want to monitor.

#### Infrastructure Monitoring

Operations Manager 2007 continues to offer comprehensive server infrastructure status monitoring and adds new features over Operations Manager 2005 to monitor SNMP-enabled devices such as routers, print servers, and computers not running Windows, even if the device or operating system does not have a Management Pack. To monitor these devices or other operating systems, you can create monitors and rules that use SNMP. A SNMP-based monitors and rules can collect data from SNMP events or traps as well as generate alerts or change the health state of the monitored object.

## Phase 4: Deploy

The Deploy phase again implements the plans derived from the effort of the previous three phases. If your organization has selected System Center Operations Manager 2007 as the technology to define and monitor your IT services, detailed deployment guidance can be found in the [online document library for System Center Operations Manager 2007 on Microsoft TechNet](http://technet.microsoft.com/en-us/library/bb310604.aspx).

## Further Information

For more information on user provisioning, go to [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) and search for “service monitoring” and “Operations Manager.”

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Defined desktop, application, and server infrastructure service models. |
|  | Evaluated technologies for monitoring availability of connections and components across defined services. |
|  | Implemented automated solution to define and monitor service levels. |

If you have completed the steps listed above, your organization has met the minimum requirement of Model-enabled service level monitoring of desktops, applications, and server infrastructure.

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

# Requirement: Quarantine Solution for Unpatched or Infected Computers

## Audience

You should read this section if you do not have a quarantine solution for unpatched or infected computers.

## Overview

In today’s security-conscious environment, an in-depth approach to protecting your network and sensitive data is a very complex matter. You can no longer rely on perimeter defenses and antivirus suites alone to protect network assets and confidential information. Security organizations and professionals now understand that internal network risks, whether intentional or accidental, have the potential to be even more perilous than external threats. To move to the Dynamic level, you need to have a mechanism for isolating unmanaged computers from your full company network.

The widespread availability of the Internet has led to significant changes in the way many organizations work. To maintain competitive advantage, organizations increasingly require employees to connect to corporate networks from remote locations such as homes, branch offices, hotels, Internet cafes, or customers' premises.

## Phase 1: Assess

The Assess phase begins the quarantine solution project by taking another inventory of client security configurations tracked in your configuration management processes. At the Dynamic level, we can assume the Standardized level requirements for best practice patch management and antivirus controls are in place as well as configuration management as part of the Rationalized level requirement set. The Assess phase examines the client configuration items and ensures that they are up-to-date.

## Phase 2: Identify

In the Identify phase, we will determine which configurations should be controlled and added to the minimum requirements for assessing whether a client computer is a threat when connecting to network resources. Typically, minimum requirements would include that all required software updates and antivirus programs are installed and signatures are up-to-date. During the Identify phase, you should also consider patch management, configuration scanning, and antivirus update practices and how these can most easily be fed into requirements of the quarantine solution to be implemented.

## Phase 3: Evaluate and Plan

In the Evaluate and Plan phase, we determine the technologies available to enable desired functionality and perform the configuration non-compliance detection and lockout routines defined in the Identify phase. The Dynamic level requires that at least remote connections to network resources be controlled via a quarantine solution. These remote connections are usually implemented with virtual private network (VPN) technologies. This section primarily references the [Implementing Quarantine Services with Microsoft Virtual Private Network Planning Guide](http://www.microsoft.com/technet/security/prodtech/windowsserver2003/quarantineservices/default.mspx) on Microsoft TechNet. We will also introduce Network Access Protection included in Windows Vista and Windows Server 2008 for on-site quarantine services.

### Virtual Private Networks (VPNs)

VPN connections allow employees and partners to connect to a corporate local area network (LAN) over a public network in a secure manner. Remote access that uses VPN technologies is a key enabler for many new business opportunities, such as remote administration and high-security applications.

Although a VPN provides secure access by encrypting data though the VPN tunnel, it does not prevent intrusions by malicious software, such as viruses or worms that initiate from the remote access computer. Virus or worm attacks can result from infected computers that connect to the LAN. VPN quarantine with the Network Access Quarantine Control features in Windows Server 2003 provides a mechanism to address these issues. VPN quarantine ensures that computers that connect to the network using VPN protocols are subject to pre-connection and post-connection checks and are isolated until the computer meets the required security policy.

The VPN quarantine solution places all connecting computers that meet the specified remote access policy into a quarantine network and verifies that these computers comply with the organization's security policy. The remote access VPN server lifts the quarantine restrictions and allows access to corporate network resources only when the remote access computer passes all connection checks.

VPN quarantine works by delaying full connectivity to a private network while examining and validating the configuration of the remote access computer against organizational standards. If the computer that connects is not compliant with the organization's policy, the quarantine process can install service packs, security updates, and virus definitions before it allows the computer to connect to other network resources.

#### VPN Quarantine Requirements

Implementing VPN quarantine requires the following components:

* Quarantine-compatible remote access clients
* Quarantine-compatible remote access server
* Quarantine-compatible Remote Access Dial-In User Service (RADIUS) server (optional)
* Quarantine resources
* Accounts database
* Quarantine remote access policy

#### Virtual Private Network Quarantine Connection Process

The following figure outlines one approach to VPN quarantine that utilizes resource servers located on a quarantine subnet.

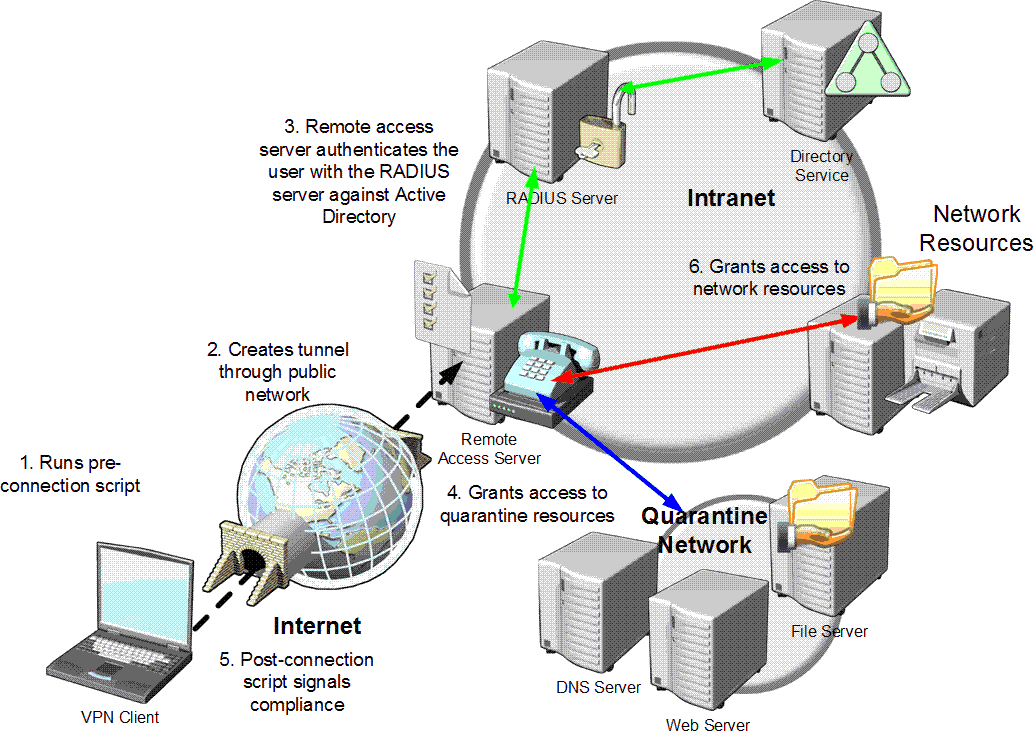


Figure 9. The VPN quarantine process path

VPN quarantine implements a modified process when the user attempts to connect to the remote network. The process includes the following steps:

1. The computer performs a pre-connection health policy validation check to ensure that the computer meets certain computer health requirements. These might include hotfixes, security updates, and virus signatures. The pre-connection script stores the results of this check locally. An organization could also run post-connection security checks if they want.
2. After the pre-connection checks have succeeded, the computer connects to the remote access server using VPN.
3. The remote access server authenticates the user credentials with the RADIUS server against the stored user name and password in the Active Directory® directory service. RADIUS is an optional component in this process.
4. If Active Directory authenticates the user, the remote access server places the client in quarantine, using the VPN quarantine remote access policy. The remote access client computer's access is limited to the quarantine resources specified by the remote access policy. Quarantine can be enforced in two possible ways on the remote access client computer: using a specific time-out period so the client computer does not stay in quarantine indefinitely or using an IP filter that restricts IP traffic to the specified network resources network only.
5. The post-connection script notifies the remote access server that the client complies with the specified requirements. If the connection does not meet the requirements in the specified time-out period, the script notifies the user and drops the connection.
6. The remote access server removes the client computer from quarantine mode by removing the IP filter and grants appropriate access to network resources specified by the remote access policy.

### Network Access Protection

[Network Access Protection (NAP)](http://www.microsoft.com/windowsserver/longhorn/network-access-protection.mspx) is a policy enforcement platform built into the Windows Vista and Windows Server 2008 operating systems that allows you to better protect network assets by enforcing compliance with system health requirements.

#### Computer Health Requirements

You are faced with the challenge of ensuring that computers that connect to and communicate on your network are compliant with system health requirements. For example, compliant computers have the correct security software installed (such as antivirus protection), the current operating system updates, and the correct configuration (such as host-based firewalls enabled). This challenge is made daunting by the portable nature of laptop computers that can roam to various Internet hotspots and other private networks, and the use of remote access connections made from home computers. If a connecting computer is not compliant, it can expose your network to attacks by malicious software such as network-level viruses and worms. To provide protection against noncompliant computers, you need to do the following:

* Centrally configure a set of policies that specify requirements for system health.
* Verify system health before allowing unlimited access to the private network or to private network resources.
* Limit the network access of noncompliant computers to a restricted network containing resources to return the noncompliant computer to a compliant state.

NAP provides components and an infrastructure that help you validate and enforce compliance with system health policies for network access and communication.

#### Health Policy Validation

When a user attempts to connect to your network, Network Access Protection validates the computer’s health state against the health policies that you have defined. You can then choose what to do if a computer is not compliant. In a monitoring-only environment, all authorized computers are granted access to the network even if some do not comply with health policies, but the compliance state of each computer is logged. In a restricted access environment, computers that comply with the health policies are allowed unlimited access to the network, but computers that do not comply with health policies or that are not compatible with Network Access Protection have their access limited to a restricted network. In both environments, computers that are compatible with Network Access Protection can automatically become compliant, and you can define exceptions to the validation process. Network Access Protection also includes migration tools to make it easier for you to define exceptions that best suit your network needs.

#### Health Policy Compliance

You can help ensure compliance with health policies by choosing to automatically update noncompliant computers with the missing requirements through management software, such as Microsoft Systems Management Server. In a monitoring-only environment, computers will have access to the network even before they are updated with required software or configuration changes. In a restricted access environment, computers that do not comply with health policies have limited access until the software and configuration updates are completed. Again, in both environments, computers that are compatible with Network Access Protection can automatically become compliant, and you can define policy exceptions.

#### Limited Network Access

You can protect network assets by limiting the access of computers that do not comply with health policy requirements. You can define the level of access noncompliant computers will have. Network access limits can be based on a specific amount of time or whether the network access is limited to a restricted network, to a single resource, or to no internal resources at all. If you do not configure health update resources, the limited access will last for the duration of the connection. If you configure health update resources, the limited access will last only until the computer is brought into compliance. You can use both monitoring and health policy compliance in your networks and configure exceptions for both.

## Phase 4: Deploy

The Dynamic level only requires that a VPN quarantine solution is implemented for remote access users. Network Access Protection solutions are recommended if your organization is using Windows Server 2008 infrastructure. [The Network Access Quarantine Control in Windows Server 2003](http://www.microsoft.com/technet/network/vpn/quarantine.mspx) guide provides additional planning and deployment guidance for quarantine solutions.

To deploy Network Access Quarantine Control, the basic steps (in order) are as follows:

1. Create quarantine resources.
2. Create a script or program that validates client configuration.
3. Install Rqs.exe on remote access servers.
4. Create a new quarantine Connection Manager (CM) profile with Windows Server 2003 Connection Manager Administration Kit (CMAK).
5. Distribute the CM profile for installation on remote access client computers.
6. Configure a quarantine remote access policy.

##### **Creating Quarantine Resources**

To allow your remote access clients to access name server, Web server, or file server resources while they are in quarantine mode, you must designate the servers and their resources that are available to remote access clients.

##### **Creating a Script or Program That Validates Client Configuration**

The quarantine script or program that you create can be an executable file (\*.exe) or as simple as a command file (\*.cmd or \*.bat). In the script, perform the set of tests to ensure that the remote access client complies with network policy.

##### **Installing Rqs.exe on Remote Access Servers**

The Remote Access Quarantine Agent service (Rqs.exe) components listen for messages from quarantine-compatible remote access clients, which indicate that their scripts have been run successfully.

##### **Creating a New Quarantine CM Profile with Windows Server 2003 CMAK**

A quarantine CM profile is just a normal remote access CM profile for dial-up or VPN access with the following additions:

* You must add a post-connect action to run the script or program you have created to check network policy compliance and include the script or program within the profile. This is done on the Custom Actions page of the CMAK Wizard.
* You must add the notification component to the profile. This is done on the Additional Files page of the CMAK Wizard.

For more information about using custom actions in CMAK, see the topic titled "Incorporating custom actions" in Windows Server 2003 Help and Support.

##### **Distributing the CM Profile for Installation on Remote Access Client Computers**

After the quarantine CM profile has been created, it must be distributed and installed on all your remote access client computers. The profile itself is an executable file that must be run on the remote access client to install the profile and configure the quarantine network connection.

##### **Configuring a Quarantine Remote Access Policy**

If Routing and Remote Access is configured with the Windows authentication provider, configure the quarantine remote access policy on the remote access server using the Routing and Remote Access snap-in. If Routing and Remote Access is configured with the RADIUS authentication provider, configure the quarantine remote access policy on the IAS server using the Internet Authentication Service snap-in.

### Summary

VPN Quarantine using Network Access Quarantine Control provides a managed way to prevent full access to your intranet until the configuration of the remote access client computer has been verified as complying with network policies. Network Access Quarantine Control uses a CM profile containing an embedded quarantine script and a notifier component, a listener component running on a Windows Server 2003 remote access server, and a quarantine remote access policy. To deploy Network Access Quarantine Control, you must designate and configure quarantine resources, create a quarantine script, install the listener component on the remote access servers, create and distribute the quarantine CM profile, and configure a quarantine remote access policy.

## Further Information

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

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Evaluated technologies to enable network quarantine for remote and on-site users. |
|  | Implemented VPN quarantine solution for remote users. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Integrated Quarantine Solution for Unpatched or Infected Computers capabilities of the Infrastructure Optimization Model.

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

Capability: Data Protection and Recovery

Data Protection and Recovery is the fourth Core Infrastructure Optimization capability. The following table describes the high-level challenges, applicable solutions, and benefits of moving to the Dynamic level in Data Protection and Recovery.

|  |  |  |
| --- | --- | --- |
| **Challenges** | **Solutions** | **Benefits** |
| **Business Challenges**  User data on individual PCs isolated from backup policy  Regulatory compliance not accomplished  **IT Challenges**  End-to-end backup process is incomplete  Disaster recovery plan is insufficient for current organizational needs | **Projects**  Implement backup and restore and defined recovery times via SLA for desktops | **Business Benefits**  Improved business continuity and availability though continuous data protection  Quick restoration of data provides a seamless working environment  Closer to implementing regulatory compliance  **IT Benefits**  Improved stability and increased productivity with data protection flexibility |

The Dynamic level in the Infrastructure Optimization Model addresses defined backup and restore procedures for desktops.

# Requirement: Backup and Restore and Defined Recovery Times via SLA for Desktops

## Audience

You should read this section if you do not have backup and restore and defined recovery times, via SLA, for 80 percent of your desktops.

## Overview

In the *Infrastructure Optimization Planning Guide for Implementers: Standardized to Rationalized* guide, you read about defining backup and restore policies for servers by establishing service level agreements (SLAs). To move to the Dynamic level, you need to apply the same concepts and services by establishing SLAs with your desktop users.

Regular backup of local hard disks prevents data loss from a disk or drive failure, disk controller errors, power outages, viruses, and other serious problems. Careful planning of backup operations and reliable equipment can make file recovery easier and faster. Using Backup in Windows XP and Windows Vista, you can back up data to tape, optical disc, or a compressed file, or you can store your backup files on a network share. In addition, there are several enterprise-class desktop backup management solutions available from Microsoft partners.

## Phase 1: Assess

During the Assess phase, examine the inventory of the desktop operating systems and device types (desktop or laptop) your organization has in production. As a requirement for previous levels in the Core Infrastructure Optimization Model, your organization should currently have Windows XP SP2 or Windows Vista operating systems on 80 percent or more of your desktop and laptop computers. An inventory in this case will be used to determine how client computers are backed-up and data restored.

## Phase 2: Identify

In the Identify phase, we will determine the goals of the backup and recovery service for desktop computers. SLAs will dictate the frequency and nature of device backups, acceptable windows between backups, necessary performance compromises, service variations between user roles, and how restore requests are processed and resolved. Automated backup schemes may vary depending on how the client computer is used, applicable laws or regulations for data processed, or sensitivity of the data processed. The identified goals should address these concerns as well as the expectations of end users.

## Phase 3: Evaluate and Plan

During the Evaluate and Plan phase, you will examine the technologies available to meet the goals identified during the previous phases. The guidance in this section is based primarily on the [Windows XP Professional Resource Kit: Backing Up and Restoring Data](http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c14621675.mspx). Windows Vista system tools for backup and restore (Backup Status and Configuration tool) are similar to those described in this guide.

### Backup Types

Deciding which type of backup to use depends on your organization’s needs. The two major considerations are the value of the data and the amount of data that has changed since the last normal or incremental backup.

The types of backup you can perform are described in the following sections.

#### Normal

A normal backup copies all selected files and marks each as having been backed up. Normal backups are the easiest to use for restoring files because you need only the most recent backup file or tape to restore all the backed-up files. Normal backups take the most time because every file that is selected is backed up, regardless of whether it has changed since the last backup.

#### Incremental

An incremental backup reduces the time required to complete the backup process by saving only files that have been created or changed since the last normal or incremental backup. It marks files so that you will know whether a specific file has been backed up. You need to create a complete normal backup of your system before you can run incremental backups. If you use a combination of normal and incremental backups to restore your data, you must have the last normal backup set of media as well as every incremental backup in chronological order since the last normal backup.

#### Differential

A differential backup can reduce the time required to complete the backup process by copying files that have been created or changed since the last normal or incremental backup. It does not mark files as backed up. You need to create a complete normal backup of your system before you run differential backups. If you use a combination of normal and differential backups, you must have the last normal backup media set and the last differential backup set to restore your data.

#### Copy

A copy backup copies all selected files, but it does not mark each copied file as backed up. Copying is a useful temporary method to back up files between normal and incremental backups; it does not affect other backup operations.

#### Daily

A daily backup copies all selected files that have been modified on the day that the daily backup is performed. The backed-up files are not marked as backed up.

Some backup types use a backup marker, also known as an “archive attribute,” to track when a file has been backed up. When the file changes, Backup marks the file to be backed up again. Files or directories that have been moved to new locations are not marked for backup. Backup allows you to back up only files with this marker set and to choose whether to mark files when they are backed up.

### Storage and Media

Windows can back up files to a variety of storage devices. Data can be backed up to tape drives, disk volumes, removable disks, and network shares, or to a library of discs or tapes in a media pool controlled by a robotic changer. If you do not have a separate storage device, back up to a local hard disk or to floppy disks.

#### Storage Devices

When you select a storage device, consider storage device and media costs, as well as reliability and capacity. Ideally, a storage device has more than enough capacity to back up the combined data of all local hard disks and can detect and correct errors during backup-and-restore operations. For information about specific storage devices, see the Windows Catalog at <http://www.microsoft.com/windows/catalog>.

#### Media Types

The most common medium is magnetic tape. Commonly used tape drives for backup include a quarter-inch cartridge, digital data storage (DDS), 8 mm cassette, Advanced Intelligent Tape (AIT), digital linear tape (DLT), and Super DLT (SDLT). High-capacity, high-performance tape drives typically use small computer system interface (SCSI) controllers. Other types of media include magnetic discs, optical discs, and CD-ROMs—recordable CD-ROM (CD-R) and rewritable CD-ROM (CD-RW).

### Establishing a Backup Plan

When you develop your backup plan:

* Keep spare hardware and media on hand in case of a failure. To avoid a problem, compare the spare hardware with the original hardware in advance to make sure that the firmware revision is the same as the original equipment.
* Test backed-up data regularly to verify the reliability of your backup procedures and equipment.
* Include stress testing of backup hardware (storage drives, optical drives, and controllers) and software (backup program and device drivers).

Several different system configurations can affect your backup strategies. At one end of the range is a simple, stand-alone computer with one user. At the other end is a workgroup network with a computer that is hosting a network public file share.

You can work out a backup solution by performing these four tasks:

1. Research and select a storage device. When considering new backup hardware, be sure to consider its reliability, speed, capacity, cost, and compatibility with your desktop operating system versions. The media must provide more than enough space to back up all your data.
2. If necessary, install a controller card in the computer. If you choose to use a SCSI-based tape drive, put the tape drive on its own controller.
3. Connect your new storage device to the computer so that you can back up the system state data. If you are using an external SCSI drive, start the drive before you start the computer so that the driver can be loaded properly.
4. Establish a backup media rotation schedule. You need to continue making backups as long as data is created or changed.

### Restoring Data

If files or directory services are not accessible, you must restore them. Restore operations are possible only if you have used Backup or another program to back up the files. Using Backup, you can restore the entire backup medium, one or more backup sets, or individual files.

## Phase 4: Deploy

The Deploy phase again implements the plans derived from the effort of the previous three phases. As with all Data Protection and Recovery scenarios, it is recommended that deployed solutions for backup and recovery be tested using periodic fire drills to ensure that procedures are functioning as intended.

## Further Information

For more information on this topic, go to the [Windows XP Professional Resource Kit: Backing Up and Restoring Data](http://www.microsoft.com/technet/prodtechnol/winxppro/reskit/c14621675.mspx) guidance on [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) or search for “backup and restore.”

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Established goals for the desktop backup and recovery service. |
|  | Defined and implemented a suitable backup and restore service for desktops in the organization and established SLAs. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for the Backup and Restore and Defined Recovery Times via SLA for Desktops of the Infrastructure Optimization Model. We recommend that you follow the guidance of additional best practice resources for backup and restore and SLAs.

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

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 Dynamic level in Security Process.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  Lacking regulatory compliance for data security  **IT Challenges**  Lack of cost/benefit analysis  Critical data may still be at risk, despite two-factor authentication  No formalized way to assess services and improve them | **Projects**  Advanced Two-Factor User Authentication  Continuous improvement programs for all security processes | **Business Benefits**  Improved information security and identity protection helps protect business from threats, regardless of device  **IT Benefits**  Proactive IT operations resolve problems earlier to avoid reducing user productivity |

The Rationalized level of optimization required that most required security measures were in place prior to moving to the Dynamic level. At the Dynamic level, all security processes should follow the lead of the ITIL/COBIT-based Management Process and participate in continuous improvement programs.

# Requirement: Advanced Two-Factor User Authentication

## Audience

You should read this section if you do not have plans in place for security policies, risk assessment, incident response, and data security.

## Overview

Most organizations know that it is important to protect their data and resources from loss or damage due to theft, human or computer error, malicious intent, or any number of other events. You can take steps to limit the opportunities for loss or damage to occur. You can also establish policies and procedures to respond to and minimize the effects of the loss or damage to your IT environment. The Dynamic level in this guide deviates somewhat from the [Core Infrastructure Optimization Online Self-Assessment](http://www.microsoft.com/business/peopleready/coreinfra/ac/default.mspx) and focuses on advanced two-factor user authentication.

At the Rationalized level, we introduced the concept of two-factor authentication, and at the Dynamic level we add to the sophistication of two-factor authentication by requiring advanced capabilities, such as biometric scanning, to access highly sensitive data.

## Phase 1: Assess

During the Assess phase, you should determine the appropriate security needs for your organization and identify which authentication processes and technologies are currently in place. Security requirements can vary dramatically from company to company or institution to institution based, for example, on size, industry or field, or regional laws and regulations. Gathering the requirements of your organization will allow you to define an appropriate security process.

## Phase 2: Identify

During the Identify phase, you will examine the tools and procedures currently in place in your organization and determine what the security requirements are for your organization. During this phase, you will gather authentication 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 Dynamic level of optimization requires strong authentication using advanced two-factor authentication, such as incorporating biometric scans, to access highly sensitive data in the organization.

### Advanced Two-Factor Authentication

Single secrets such as passwords can be effective security controls. A long password of more than 10 characters that consists of random letters, numbers, and special characters can be very difficult to crack.

Advanced two-factor authentication systems overcome the issues of single secret authentication by the requirement of a second secret. Advanced two-factor authentication uses a combination of two of the following three items:

* Biometrics, such as retina or fingerprint scans, and/or
* Something the user knows, such as a personal identification number (PIN) and/or
* Something that the user has, such as a hardware token or a smart card.

Biometrics can be excellent authentication mechanisms. Examples of biometric measurements include retinal scans, facial feature scans, palm prints, fingerprints, and voice recognition. With biometrics, users may or may not need to enter user IDs, but they are clearly authenticated with features that only they possess. Organizations can provide an important additional layer of security if they implement biometrics for strong authentication. For detailed information on two-factor authentication, go to <http://www.microsoft.com/technet/security/guidance/networksecurity/securesmartcards/default.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 that data processes are efficient.

## Further Information

For more information on developing security operations and process standards, go to the Security Guidance Portal on Microsoft TechNet at <http://www.microsoft.com/technet/security/guidance>.

## Checkpoint: Advanced Two-Factor User Authentication

|  |  |
| --- | --- |
| X | Requirement |
|  | Developed and implemented advanced two-factor identity and access management policies for highly sensitive data. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for Advanced Two-Factor User Authentication.

We recommend that you follow additional best practices for security processes addressed at the [Microsoft TechNet Security Center](http://www.microsoft.com/technet/security/default.mspx).

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

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 Dynamic level in ITIL/COBIT-based Management Process.

|  |  |  |
| --- | --- | --- |
| Challenges | Solutions | Benefits |
| **Business Challenges**  Lacking knowledge of IT service costs and benefits  IT staffing, development, and retention models not in place  **IT Challenges**  Infrastructure engineering lacks known standards | **Projects**  Implement availability management procedures  Improve financial management of IT services  Standardize infrastructure engineering processes  Formalize IT service continuity management  Implement best practice workforce management | **Business Benefits**  Cost structure of IT services is known and managed  IT staffing is more stable  Plans in place to maintain service continuity  **IT Benefits**  IT investments are easier to validate  Knowledge is preserved in the IT organization |

The Dynamic level of optimization requires that your organization has defined procedures for availability management, financial management, infrastructure engineering, IT service continuity management, and workforce management. In addition to these new disciplines, the Dynamic level carries the expectation that all IT services participate in continuous improvement programs and are regularly assessed and improvements are made according to business or organizational needs.

# Requirement: Optimizing Processes

## Audience

You should read this section if you do not have formalized processes for financial management, availability management, IT service continuity management, workforce management, security management, or infrastructure engineering.

## Overview

Infrastructure optimization goes beyond products and technologies. People and processes compose a large portion of an organization’s IT service maturity. A number of standards and best practice organizations address the areas of people and process in IT service management. [Microsoft Operations Framework (MOF)](http://www.microsoft.com/mof) applies much of the knowledge contained in the [IT Infrastructure Library (ITIL)](http://www.itil.co.uk/) and [Control Objectives for Information and related Technology (COBIT)](http://www.isaca.org/) standards and makes them actionable and achievable for Microsoft customers.

## Phase 1: Assess

The goal of the Assess phase in operations management is to evaluate the organization’s current capabilities and challenges. To support the operations assessment process, Microsoft has developed the Microsoft Operations Framework (MOF) Service Management Assessment (SMA) as part of the [MOF Continuous Improvement Roadmap](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/index.mspx), and a lighter online version called the [MOF Self-Assessment Tool](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/moftool.mspx).

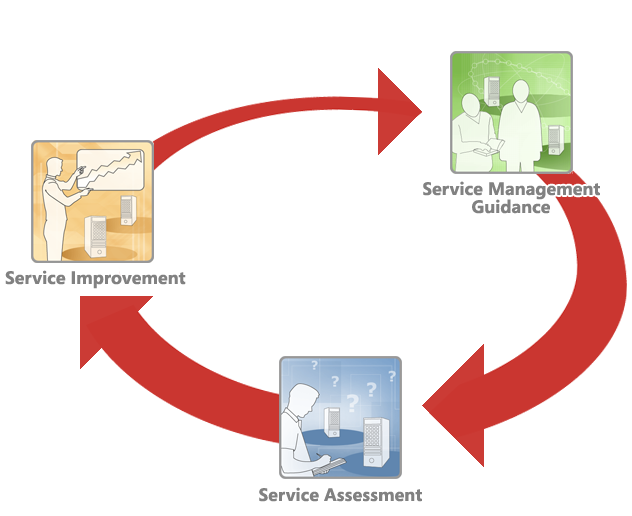


Figure 10. MOF Continuous Improvement Roadmap

The MOF Service Management Assessment is focused on enhancing the performance of people and IT service management processes, as well as enabling technologies that improve business value. All recommendations generated as a result of the SMA are detailed and justified in business value, and a detailed service improvement roadmap is provided, supported by specific key performance indicators to monitor progress as improvements are implemented.

## Phase 2: Identify

The results of the MOF Service Management Assessment form the basis of the Identify phase. The Assessment will often expose several areas of potential improvement in IT operations. During the Identify phase, we consider these results and prioritize improvement projects based on the business need. Tools and job aids are included in the MOF Continuous Improvement Roadmap to assist with this prioritization.

## Phase 3: Evaluate and Plan

The Evaluate and Plan phase for operational improvement relies on the identified and prioritized areas for improvement. The MOF Service Improvement Program (SIP) guidance enables this phase. SIP is split into two major areas of focus: specific MOF/ITIL process improvement and service improvement guidance. This guidance is delivered through a tool that assists users in identifying their specific trouble points, provides focused guidance for remediation, and is supported by key performance indicators to measure process improvement.

### Recommended Processes for Moving to the Dynamic Level

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

The Rationalized level begins to incorporate measures for predictability and can be evaluated based on predefined targets. In order to enable performance tracking, IT operations have reached a proactive state of control with a focus on monitoring. At the rationalized level, the IT operation is on par with other business operations and, therefore, has similar accountability for performing against pre-defined service level agreements. Accountability and measurability also mean that management expects the IT operations to improve at the same level as other business operations.

The Dynamic level goes to the final step where IT becomes a leading business operation. At this stage, the IT operation has in-depth knowledge of activity-based costing and can accurately predict the impact of each additional investment. This predictability allows the IT operation the freedom to determine where resources are allocated. Monitoring, operating, and changing procedures are seamless, allowing for maximized agility and continuous operational improvement through advanced automation.

Microsoft provides [Microsoft Operations Framework (MOF)](http://www.microsoft.com/mof) as an iterative model for defining and improving IT operations. MOF defines service management functions (SMFs) as logical operational functions within an IT organization. The SMFs are grouped together into four broad areas: Changing, Operating, Supporting, and Optimizing. This guide highlights areas to improve that are typically found in organizations at the Rationalized level of optimization:

* [Availability Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx)
* [Financial Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smffinmg.mspx)
* [Infrastructure Engineering](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfinfeng.mspx)
* [IT Service Continuity Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsrcmg.mspx)
* [Workforce Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfwrkmg.mspx)

These SMFs represent the MOF Optimizing Quadrant and are the remaining topics for process improvement. Optimizing SMFs omitted from this discussion are Service Level Management, Security Management, and Capacity Management since they were requirements for the Rationalized level and were discussed as a requirement for the Desktop, Device and Server Management capability previously in this guide.

Depending on the organization, improvements to these service management functions might or might not have the greatest impact on operational effectiveness and improvement. We recommend that your organization at a minimum completes the [online self-assessment](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/moftool.mspx), and preferably a full [Service Management Assessment](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/index.mspx), to identify the most important areas requiring process or service improvements.

## Phase 4: Deploy (Availability Management)

[Availability management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx) is concerned with the design, implementation, measurement, and management of IT infrastructure availability to ensure that stated business requirements for availability are consistently met. In particular:

* Availability management should be applied to all new IT services and for established services where service level requirements (SLRs) or service level agreements (SLAs) are established.
* Availability management can be applied to IT services that are defined as critical business functions, even when no SLA exists.
* Availability management can be applied to the suppliers (internal and external) that form the IT support organization as a precursor to the creation of a formal SLA.
* Availability management considers all aspects of the IT infrastructure and supporting organization that may affect availability, including training, skills, policy, process effectiveness, procedures, and tools.

The Availability Management SMF consists of three main processes and a number of subprocesses. In order to deploy best practice Availability Management, the following tasks and processes should be followed:

* Define service level requirements.
* Define critical customer functions.
* Define availability objectives.
* Propose availability solution.
* Identify major IT service components
* Design for availability.
* Availability risks and countermeasures.
* Life cycle management needs.
* Design for recovery.
* Incident life cycle.
* Designing for customer satisfaction during outages.
* Management processes.
* Formalize operating level agreements.

For more detailed information on each task and process, see the [Microsoft Operations Framework Availability Management Service Management Function](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfavamg.mspx).

## Phase 4: Deploy (Financial Management)

The objective of the [financial management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smffinmg.mspx) process is the sound management of monetary resources in support of organizational goals. Financial data provides the expense, or cost, side of the equation for making business decisions regarding changes in the IT infrastructure, systems, staffing, or processes. A properly functioning financial management process helps IT managers to make better-informed decisions for IT planning and investment.

The goals and objectives of financial management are to be able to fully account for the cost of IT services, to attribute the costs to the services delivered to the organization’s customers so that the costs can be recovered, to aid in decision making by understanding the cost of IT services, and to provide business cases for changes to IT services based on a sound understanding of the costs involved.

Proper financial management of the IT department provides management with visibility of computing costs. Cost visibility provides benefits including:

* IT provides services within budgets that are negotiated with customers.
* The costs of providing an agreed-to level of service are trackable and understandable.
* The IT department can trace costs and report the origin of costs to customers and executive management.
* Customers are fairly charged for the services being provided and the prices charged are more predictable.
* The IT department is able to compare the cost of providing services to the costs charged by outside vendors.
* Accurate cost data will assist the business unit in the preparation of accurate and realistic bids and proposals.
* Accurate cost data is necessary to optimize operations.

Successful implementation of best practice financial management comprises four main processes and a number of subprocesses, which are listed below.

**Cost accounting**

* Service level agreements
  + Service level agreement and financial management
  + Tracking performance
  + Renegotiating the service level agreement
  + Components of a service level agreement
* Cost classification
* Setting up accounts
* Capital costs
* Operational costs
* Direct costs
* Indirect costs
* Fixed costs versus variable costs
* Cost categorization
* Cost units
* Depreciation
* Cost accounting methods
  + Cost-by-customer accounting method
  + Cost-by-service accounting method
  + Activity-based costing
  + Request for change review and approval

**Project investment appraisals**

* Net present value
* Payback period
* Return on investment
* Total cost of ownership
* Real cost of ownership (RCO)
* Measurement
* Management
* Managerial reports

**Budgeting**

* Budgeting benefits
* Budget inputs
  + Service level agreements
  + Customer requirements
  + Internal cost inputs
  + Trends
* Budget types
* Operating budget
* Capital budget
* Budgeting methods
  + Prior year budgeting
  + Zero-based budgeting
* Budget review

**Cost recovery**

* Transfer pricing methods
  + At cost
  + Cost plus
  + Flat rate plus premium
  + Market rate
* Billing

For more detailed information on each task and process, see the [Microsoft Operations Framework Financial Management Service Management Function](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smffinmg.mspx).

## Phase 4: Deploy (Infrastructure Engineering)

Consistent standards across an IT organization improve interoperability, reduce risk of deployment failures, and facilitate governance. [Infrastructure Engineering](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfinfeng.mspx) (IE) is the process of collecting, creating, and managing standards and policies for IT services and infrastructure. Through implementation of the Infrastructure Engineering formalized processes, organizations will:

* Develop standards, policies, benchmarks, and guidelines for managing the infrastructure now and in the future, maximizing availability, supportability, and operability.
* Provide guidance and control to ensure that solutions are operable at the appropriate level and to optimize timing for new solution design and changes.
* Ensure that the infrastructure in use, including the technology and common application portfolios (for example, standard desktops) align to the business strategy and direction.
* Measurably improve their management of the infrastructure environment.
* Provide for a means of verifying quality assurance (QA) for all infrastructure development at the planning and authorization stages.
* Maintain a cost-aware approach to the selection of strategic technology solutions and reduce unnecessary costs.

Infrastructure Engineering will take the lead in identifying and normalizing existing standards and policies and determining the need for new ones. The IE SMF has responsibility for managing the development of standards and policies, typically through internal or external subject matter experts.

An organization that implements best practice Infrastructure Engineering should have the organizational capabilities in place to be able to complete and maintain the following:

* Discover current standards and policies.
* Define categories of standards, processes, and policies that align with their IT organizational structure.
* Define an effective suite of standards, processes, and policies for common IT activities.
* Implement and maintain a change management process.
* Apply the standards and policies for design, development, and deployment tasks.

The breadth and depth of the standards and policies that are developed and applied may vary from organization to organization, depending upon the maturity level to which other MOF service management functions have been adopted.

In implementing the Infrastructure Engineering process, a setup activity is initiated to define the scope of the infrastructure environment and to determine how best to manage it using defined policies and standards. Regulation of the infrastructure through the use of these standards can be as passive or active as the organization needs, although it is suggested that the use of established policies and standards be enforced at the Change Initiation Review, as a minimum.

### Infrastructure Engineering Process Flow

The development and application of consistent IT policies and standards across an organization is accomplished through the following process, which is described in detail in subsequent sections.

#### Define the Infrastructure Environment

A clear and thorough definition of the infrastructure environment is key to its successful and subsequent management. This process provides guidance on how to define the environment and determine the desired scope of environmental components to be regulated. It also examines how to categorize elements of the infrastructure into sensible groupings to allow effective utilization of standards and policies.

#### Collect and Define Policies and Standards

The use of policies and standards to control evolution of the infrastructure helps to maintain a stable and effectively aligned IT organization. This process provides guidance on collecting and documenting the policies and standards that exist across the infrastructure and defining new ones where necessary, looking in particular at key inputs that will ensure the best fit for the organization now and several years into the future.

#### Apply Policies and Standards for Infrastructure Guidance

The creation of policies and standards adds real value only if they are used effectively to provide guidance and control over the integrated infrastructure environment. This process examines how policies and standards should be applied in developing a new requirement or a change to the infrastructure. The process also describes an alternative for dealing with situations that fall outside the need for a standard or policy by taking a controlled approach to exceptions.

#### Maintain Policies and Standards

Because the policies and standards are created across all the processes and IT personnel roles, it is important to ensure that they are maintained effectively and kept accessible to all potential users.

For more detailed information on Infrastructure Engineering, see the [Microsoft Operations Framework Infrastructure Engineering Service Management Function](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfinfeng.mspx).

## Phase 4: Deploy (IT Service Continuity Management)

Major IT outages occur outside the realm of availability and incident management. [IT Service Continuity](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsrcmg.mspx) provides best practices and guidance to support business continuity through the implementation of effective IT service recovery procedures.

Many factors affect the availability of an IT service such as hardware failure, environmental issues, and human error. A hardware failure, such as a broken power supply or disk drive, is one of the most obvious factors to consider. If the only power supply to a server fails, then this might cause the whole IT service to be lost. Dual redundant power supplies attached to the server can be employed to mitigate some of this risk. If power to the whole computer room or data center is disrupted, battery backup systems can be employed to cover the short time it might take to start up a standby generator. Exposures such as these are referred to as availability risks and the actions we might take to mitigate them are called countermeasures.

Risks to availability also exist within processes and procedures and also arise out of human error. If a poorly tested change is introduced that inadvertently prevents users from connecting to the IT service, then the complete service is unavailable until access is restored. If the production database is accidentally overwritten with last night's backup data instead of a new backup being performed, this can have catastrophic consequences on availability. Countermeasures, such as carefully designed testing and release procedures and appropriate staff training plans, can also be employed to help mitigate these risks. When these mitigation plans fail, contingency plans must be invoked.

Availability management and service continuity management are closely related in this respect as both processes strive to eliminate risks to the availability of IT services. The prime focus of availability management is handling the routine risks to availability that can be reasonably expected to occur on a day-to-day basis. Where no straightforward countermeasures are available or where the countermeasure is prohibitively expensive or beyond the scope of a single IT service to justify in its own right, these availability risks are passed on to service continuity management to handle.

Service continuity management is concerned with managing risks to ensure that an organization's IT infrastructure can continue providing services in the event of an unlikely or unanticipated event. This is accomplished through a process that analyzes business processes, their impact on the organization, and the IT infrastructure vulnerabilities that these processes face from a myriad of possible risks. This requires a great deal of research to be conducted with diligence to identify all critical business processes and their vulnerabilities.

This task begins by dividing the effort into three phases: define the service level objectives, propose a solution to meet those objectives, and formalize the written agreements and contingency plan. Each phase has tasks and deliverables associated with it that assists in determining cost-effective solutions. The deliverables need to be maintained as active documents and updated as needed.

Service continuity management consists of four main processes and a number of subprocesses as described in the following list.

**Acquire service level requirements**

* Identify information technology service layers
  + Service
  + Application
  + Middleware
  + Operating system
  + Hardware
  + Local area network
  + Passive components
  + Hubs, switches, and routers
  + Network interface cards
* Facilities
* Edifice
* Environmental controls
* Physical security
* Fire suppression
* Human convenience
* Egress
  + Security
  + Water
  + Sewage
  + Gas
  + Electricity
  + Internet access
* Identify risks to each information technology service layer

**Propose contingent solution**

* Design for failover
* Outsourced services
* Facilities

**Formalize operating level agreements**

**Formalize the contingency plan**

* Definition of contingency levels
* Escalation and notification procedures
* Startup and shutdown procedures
* Communications methods
* Status reporting requirements

For more detailed information on IT Service Continuity Planning and associated operator role clusters, see the [Microsoft Operations Framework Service Continuity Planning Service Management Function](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfsrcmg.mspx).

## Phase 4: Deploy (Workforce Management)

Skilled IT personnel are crucial to the evolution of an efficient IT organization. Their recruitment, training, readiness, compensation, and retention are discussed as part of [Workforce Management](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfwrkmg.mspx). Best practice workforce management should be observed at all levels of optimization; it becomes a defined discipline at the Dynamic level, meaning that the success of defined goals in workforce management are tracked and measured to ensure continuous improvement.

Key goals and benefits of workforce management include:

* Correct staffing levels to meet the needs of the computer production environment and the business needs.
* Staff with the appropriate level of technical skills.
* Retention of staff.
* A reduction in absence due to stress and sickness.
* Skill sets suitable for coping with a changing environment, products, and services.
* Clear and well-understood career paths and growth opportunities.
* Ability to absorb contract staff seamlessly.
* An ergonomic working environment.

Workforce management is concerned with recruiting and retaining staff to meet the needs of the operations organization. This is dependent upon the size, IT architecture, and the specialized needs and sophistication of the organization. It is also dependent on the organizational model implemented within the organization.

### Workforce Management Considerations

#### Staffing Levels and Skill Sets

Once the IT architecture and specialist needs are understood, then workforce management must understand the business needs, based on the SLA and the computing requirements of the organization, before it can establish the correct level of staffing requirements. Understanding the correct staffing and skill levels needed is an ongoing process so that staff or skill shortages do not occur unexpectedly.

Hiring the right staff who possess the appropriate skill sets and who will work well as part of a team is the main responsibility of the human resources manager.

Having the right staff with the appropriate skill sets can be achieved by ensuring that staff members are rewarded for their contributions. In addition, providing excellent training schemes (training profiles should exist for each job description), certification programs, and enhanced career prospects and career paths increases hiring success. (Such policies and programs should be established before problems arise and staff loses occur.)

One of the most critical (and most often neglected) aspects of managing a workforce is the process of conducting an ongoing skills inventory of the staff. Taking a regular inventory of current skill sets across the operations workforce helps identify areas of weakness.

#### Employee Retention

A stable workforce is crucial to maintaining service levels. Employee retention is the cornerstone of workforce stability. It also leads to increased productivity over time and improved customer service. An effective workforce plan is therefore needed to retain employees (reduce turnover) by using proactive retention techniques that give the employee incentives to remain in the workforce. Hiring the right people is of no value if the organization cannot retain them over time.

#### Employee Absence

The human resources manager should use consistent attendance management policies to deal effectively with unplanned absence. The policies should clearly define expectations of attendance and proper notification procedures, as well as the disciplinary measure(s) that will be taken against staff who are absent beyond tolerable limits. In order for this policy to be credible and successful, it needs to be communicated to all staff and applied uniformly throughout the organization.

Absence can be planned or unplanned and may not necessarily reflect poor health by the person who is absent. Whether planned or unplanned, employee absence has a detrimental effect on the services provided by the entire workforce to the organization. Nevertheless, employee absence is a reality in any workforce and needs to be accepted and planned for.

#### Performance Management

The human resources manager must develop a high-quality performance management system for the support staff by giving them specific goals to attain—goals that are measurable, appropriate, and fully support the SLAs. He or she must ensure that all employees understand the goals and that the employees obtain feedback in order to develop their goals.

#### Environment

The workplace environment can play an important role in the retention of service and support staff. Since personnel availability is key to the success of an efficient and service-oriented workforce, employees are often required to stay at their workstations for extended periods. A functional workspace that provides for elements like acoustic balance, ergonomic workstations, and an efficient and clean overall atmosphere increases employee satisfaction and their feelings of "wanting to be there."

#### External Resources

Contracted resources may form part of a short- or long-term staff augmentation; familiarizing them with company policies and procedures provides a seamless and trouble-free staff augmentation experience.

It is the responsibility of the human resources manager to ensure that every support professional, whether internal or external, has a clear understanding of the support organization's goals, processes and procedures, tools, success and measurement metrics, and measurement process.

### Workforce Management Processes

Workforce management consists of six main processes and a number of subprocesses, which are described in the following list.

**Crafting an operations organization**

* Determining staffing requirements
  + Operations organization makeup considerations
  + Predicting staffing levels
* Hiring and retention considerations
* Attracting, developing, and keeping strong IT operations staff
* Proper employee orientation
* Job descriptions
* Workforce skills assessment
* Workforce retention management
* Workforce absence control

**Workforce performance considerations**

* Individual and group objective setting
* Performance monitoring and metrics
* Performance measurement
* Performance evaluation
* Reward and recognition considerations

**Considerations for external resources**

**Maintaining a ready and reliable workforce**

* Employee readiness considerations
* Operations professional training considerations
* Balancing training with support requirements
* Environmental considerations

**Employee safety**

For more detailed information on Workforce Management, see the [Microsoft Operations Framework Workforce Management Service Management Function](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/smf/smfwrkmg.mspx).

## Further Information

For more information on this topic, go to the [Microsoft Operations Framework Optimizing Quadrant](http://www.microsoft.com/technet/solutionaccelerators/cits/mo/mof/mofoptimize.mspx) guidance on [Microsoft TechNet](http://technet.microsoft.com/en-us/default.aspx) or search for “MOF Optimizing.”

## Topic Checkpoint

|  |  |
| --- | --- |
| X | Requirements |
|  | Implemented best practice Availability Management. |
|  | Implemented best practice Financial Management. |
|  | Implemented best practice Infrastructure Engineering. |
|  | Implemented best practice IT Service Continuity Management. |
|  | Implemented best practice Workforce Management. |

If you have completed the steps listed above, your organization has met the minimum requirement of the Dynamic level for the ITIL/COBIT-based Management Process capability of the Infrastructure Optimization Model.

Additional Resources: Tools and Technologies

The following table lists the recommended tools, technologies, and services for moving from the Rationalized to the Dynamic 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. |
| [Active Directory Federation Services (ADFS)](http://technet2.microsoft.com/WindowsServer/f/?en/library/1f6e9e6e-c179-4dd2-bd1d-c74dd4ebf56b1033.mspx) | ADFS is a component in Microsoft Windows Server 2003 R2 that provides browser-based clients (internal or external to your network) with single sign-on (SSO) access to protected Internet-facing applications, even when the user accounts and applications are located in completely different networks or organizations. |
| [Antivirus Software](http://www.microsoft.com/athome/security/viruses/wsc/en-us/flist.mspx) | Antivirus software is specifically designed to detect and prevent viruses. |
| [Application Compatibility Toolkit](http://technet.microsoft.com/en-us/windowsvista/aa905102.aspx) | The Microsoft Application Compatibility Toolkit (ACT) is a life-cycle management tool that assists in identifying and managing your overall application portfolio and help resolve application compatibility issues. |
| [Business Desktop Deployment 2007 (BDD 2007)](http://www.microsoft.com/technet/desktopdeployment/bdd/2007/default.mspx) | A solution accelerator from Microsoft that provides comprehensive guidance and tools to manage large-scale desktop deployment projects, ongoing image management, and new-user desktop provisioning. |
| [Group Policy](http://technet2.microsoft.com/windowsserver/en/technologies/featured/gp/default.mspx) | Group Policy is an infrastructure used to deliver and apply one or more desired configurations or policy settings to a set of targeted users and computers within an Active Directory environment. |
| [Microsoft Identity Integration Server (MIIS)](http://www.microsoft.com/technet/miis/default.mspx) | MIIS creates and distributes an integrated view of identity information from multiple data sources. |
| [Identity Lifecycle Management Server (ILM)](http://www.microsoft.com/windowsserver/ilm2007/default.mspx) | ILM brings together metadirectory, certificate management, and user provisioning into one solution that works across Windows and other enterprise systems. |
| [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. |
| [Microsoft Virtual Server](http://www.microsoft.com/technet/virtualserver/default.mspx) | Provides a virtualization platform that runs most major x86 operating systems in a guest environment and is supported by Microsoft as a host for Windows Server-based operating systems and Windows Server System™ applications. |
| [Microsoft Systems Management Server (SMS)](http://www.microsoft.com/technet/sms/default.mspx) | SMS is a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to quickly and cost-effectively provide relevant software and updates to users from Microsoft and non-Microsoft vendors. |
| [SMS 2003 Desired Configuration Monitoring](http://www.microsoft.com/downloads/details.aspx?FamilyID=a867fc14-daa3-4c2a-9e65-4fbcbec60aaa&DisplayLang=en) | SMS 2003 Desired Configuration Monitoring enables you to define customized configuration standards for desktops and servers and then perform automated compliance audits against defined configuration standards. |
| [System Center Operations Manager](http://www.microsoft.com/technet/opsmgr/default.mspx) | System Center Operations Manager 2007 is the next version of Microsoft’s event and performance monitoring solution, Microsoft Operations Manager. Operations Manager 2007 improves on the functionality of its predecessor by extending monitoring to IT services and desktop clients. |
| [System Center Configuration Manager](http://www.microsoft.com/technet/sms/default.mspx) | System Center Configuration Manager 2007 provides a comprehensive solution for change and configuration management for the Microsoft platform, enabling organizations to provide relevant software and updates to users quickly and cost-effectively. |
| [System Center Virtual Machine Manager](http://www.microsoft.com/systemcenter/scvmm/default.mspx) | System Center Virtual Machine Manager provides centralized administration of virtual machine infrastructure and enables increased physical server utilization and rapid provisioning of new virtual machines by the administrator and authorized end users. |
| [Virtual Private Networks (VPN)](http://www.microsoft.com/technet/network/vpn/default.mspx) | A VPN encompasses links across shared or public networks. VPN connections use the connectivity of the Internet plus a combination of tunneling and data encryption technologies—such as the Point-to-Point Tunneling Protocol (PPTP) and Layer Two Tunneling Protocol with Internet Protocol security (L2TP/IPsec) to connect remote clients and remote offices. |
| [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 Vista](http://www.microsoft.com/windows/products/windowsvista/default.mspx) | Windows Vista is the latest desktop operating system from Microsoft. Feature improvements have been made to deployment and management, desktop search, mobility, and security. |
| [Windows Vista Hardware Assessment](http://go.microsoft.com/fwlink/?LinkID=86625) | Windows Vista Hardware Assessment is an agentless tool that makes it easier for customers and consultants to inventory and assess a PCs’ readiness for Windows Vista migration across networks regarding hardware and device driver compatibility. |
| [Zero Touch Provisioning (ZTP)](http://www.microsoft.com/technet/desktopdeployment/bdd/enterprise/ZTPDFTGuide_1.mspx) | ZTP allows organizations to move to a managed, self-service provisioning portal that allows delegates to perform common provisioning tasks, such as password resets, e-mail provisioning, and elective application installation. ZTP is based on Microsoft BizTalk Server and requires the use of Systems Management Server 2003. |

# 

Additional Resources: Rationalized to Dynamic Checklist

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

## Capability: Identity and Access Management

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Centralized automated user account provisioning (for example, issuing new accounts, changing passwords, synchronizing permissions, enabling access to business applications) across 80 percent or more of heterogeneous systems.** |  |  |
| Attributes:   * Defined current identity object provisioning workflows in your organization, as well as areas to improve or optimize. * Identified technologies used to manage object identity life cycles. * Implemented a consolidated solution to automate common user account provisioning workflows. | | |
| Requirement 2 | Yes | No |
| **Implemented a federated directory-based tool to enable authenticated access to external customers, service providers, and business partners.** |  |  |
| Attributes:   * Validated need for providing authenticated access to external entities. * Determined strategies and policies for providing external access to defined resources. * Implemented technologies to ensure secure access for defined external users to defined services. | | |

## Capability: Desktop, Device and Server Management

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Tools in place to perform automated infrastructure capacity planning for primary IT services (such as e-mail).** |  |  |
| Attributes:   * Identified primary IT service candidates for automated capacity planning. * Created capacity models to automate capacity planning or implemented capacity planning tools. | | |
| Requirement 2 | Yes | No |
| **Management of mobile devices and access to IT services and applications nearly at parity with managed desktop and laptop computers.** |  |  |
| Attributes:   * Implemented secure technologies to provide access to primary line-of-business applications (for example, LOB apps, CRM, supply chain) via mobile devices. * Established defined set of standard basic images for mobile devices. * Implemented an automated solution to continuously update configuration settings and/or applications in mobile devices. * Deployed an automated quarantine solution for mobile devices. * Implemented an automated patch management solution for mobile devices. * Implemented an automated asset management solution for mobile devices. | | |
| Requirement 3 | Yes | No |
| **Implemented virtualization to dynamically move workloads from server to server based on resource needs or business rules.** |  |  |
| Attributes:   * Deployed a subset of production IT services or applications to virtual machines. * Actively managing and optimizing system resources on shared hardware devices. | | |

## Capability: Security and Networking

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Integrated threat management and mitigation across clients and server edge.** |  |  |
| Attributes:   * Assessed server edge security threats and evaluated threat mitigation solutions. * Implemented technology solutions to protect against Internet-based threats across the client and server edge. | | |
| Requirement 2 | Yes | No |
| **Model-enabled service level monitoring of desktops, applications, and server infrastructure.** |  |  |
| Attributes:   * Defined desktop, application, and server infrastructure service models. * Evaluated technologies for monitoring availability of connections and components across defined services. * Implemented automated solution to define and monitor service levels. | | |
| Requirement 3 | Yes | No |
| **Automated quarantine solution for unpatched or infected computers.** |  |  |
| Attributes:   * Evaluated technologies to enable network quarantine for remote and on-site users. * Implemented VPN quarantine solution for remote users. | | |

## Capability: Data Protection and Recovery

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Implemented defined backup and restore services with service level agreements for 80 percent or more of desktops.** |  |  |
| Attributes:   * Established goals for the desktop backup and recovery service. * Defined and implemented a suitable backup and restore service for desktops in the organization and established SLAs. | | |

### Capability: Security Process

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Established security processes and technologies to enable advanced two-factor user authentication (such as biometric scans) for highly sensitive data.** |  |  |
| Attributes:   * Developed and implemented advanced two-factor identity and access management policies for highly sensitive data. | | |

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

|  |  |  |
| --- | --- | --- |
| Requirement 1 | Yes | No |
| **Implemented best practices for further optimizing your IT organization.** |  |  |
| Attributes:   * Implemented best practice Availability Management. * Implemented best practice Financial Management. * Implemented best practice Infrastructure Engineering. * Implemented best practice IT Service Continuity Management. * Implemented best practice Workforce Management. | | |