

How Essential Business Server Meets Core Infrastructure Optimization Capabilities and Attributes

Microsoft Corporation

Published: April 2009

Version: 1

Abstract

The Microsoft Infrastructure Optimization Model (explained later in this document) provides a framework for evaluating your current and planned IT infrastructure. A standard out-of-the-box installation of Windows Essential Business Server (EBS) helps you implement the vision of an optimized information technology infrastructure in your midsize business. This document examines each of the five capabilities and associated attributes and explains which capabilities and attributes are met by a standard deployment of EBS and which attributes require further customization.

For information about Essential Business Server, go to:

http://www.microsoft.com/ebs

For the latest information and for more detailed descriptions and business benefits of the Microsoft Infrastructure Optimization Model, go to:

http://www.microsoft.com/technet/infrastructure.

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

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

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

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

© 2009 Microsoft Corporation. All rights reserved. This work is licensed under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, United States.

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

All other trademarks are property of their respective owners.

Contents

[Overview 1](#_Toc227797157)

[Evaluate Your Organization’s Current Maturity Level 1](#_Toc227797158)

[Prepare and Plan for Essential Business Server 2](#_Toc227797159)

[Core Infrastructure Optimization Overview 2](#_Toc227797160)

[Audience 2](#_Toc227797161)

[Infrastructure Optimization Concept 3](#_Toc227797162)

[Core Infrastructure Optimization Capabilities 4](#_Toc227797163)

[Identity and Access Management 4](#_Toc227797164)

[Desktop, Device and Server Management 4](#_Toc227797165)

[Data Protection and Recovery 4](#_Toc227797166)

[Security and Networking 4](#_Toc227797167)

[IT and Security Process 5](#_Toc227797168)

[Core Infrastructure Optimization Model Levels 5](#_Toc227797169)

[Optimization Level 1: Basic, "We Fight Fires" 5](#_Toc227797170)

[Optimization Level 2: Standardized, "We're Gaining Control" 5](#_Toc227797171)

[Optimization Level 3: Rationalized, "We Enable Business" 5](#_Toc227797172)

[Optimization Level 4: Dynamic, "We're a Strategic Asset" 6](#_Toc227797173)

[Core Infrastructure Optimization Capability Overview 7](#_Toc227797174)

[How Essential Business Server Implements Core IO 8](#_Toc227797175)

[Identity and Access Management 9](#_Toc227797176)

[Desktop, Device, and Server Management - Standardized 12](#_Toc227797177)

[Security and Networking 20](#_Toc227797178)

[Data Protection and Recovery 25](#_Toc227797179)

[IT and Security Process 27](#_Toc227797180)

[Appendix A – Detailed Description of Capabilities 32](#_Toc227797181)

[Identity and Access Management 32](#_Toc227797182)

[Desktop, Device, and Server Management 33](#_Toc227797183)

[Security and Networking 35](#_Toc227797184)

[Data Protection and Recovery 38](#_Toc227797185)

[IT and Security Process 39](#_Toc227797186)

[Appendix B – Additional resources 40](#_Toc227797187)

[Appendix C – Assumptions 41](#_Toc227797188)

Overview

Windows Essential Business Server (EBS) 2008 is an enterprise-class server solution designed and priced for midsize businesses with up to 300 users and 30 servers. Windows Essential Business Server 2008 provides a unified Administration Console to manage an integrated IT infrastructure with the latest versions of management, messaging, and security server technologies. By helping to improve IT manageability and reliability, Windows Essential Business Server 2008 turns a midsize IT infrastructure into a strategic asset, boosting productivity and growth. Turning IT infrastructure into a strategic asset is the endpoint and objective of the Microsoft Core Infrastructure Optimization (Core IO) Model.

Core IO (explained later in this document) provides a framework for evaluating your current and planned IT infrastructure. Core IO is divided into four levels--Basic, Standardized, Rationalized, and Dynamic—each with their own set of capabilities and attributes. This document examines each of the five capabilities, associated attributes, and explains which capabilities and attributes are met by a standard deployment of EBS.

# Evaluate Your Organization’s Current Maturity Level

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

Two tools are available for you to assess your organization’s current maturity level. The first tool, a self-assessment tool (http://www.microsoft.com/infrastructure/about /gettingstarted.mspx) consisting of nine questions, provides a customized report that shows where your organization is for each of the Core IO capabilities. Your results are compared with others who have completed the assessment in your industry. Use the report as a high-level overview for how to further optimize your organization’s infrastructure.

The second assessment tool (http://www.microsoft.com/optimization/tools/ overview.mspx) provides a more detailed, comprehensive report that serves as a roadmap for optimizing your IT infrastructure. This tool also helps identify specific IT projects that can lead to immediate cost savings.

After completing the assessment you will have a benchmark of how your organization has implemented the Core IO model. You will have identified areas that need optimization. Use this document to understand how deploying Essential Business Server fills those optimization needs. The next step is to prepare and plan for the EBS Installation.

# Prepare and Plan for Essential Business Server

Additional helpful tools for assessment are the Preparation and Planning   
Wizards. The tools are designed to help you perform the preparation and planning steps to deploy EBS. The planning and preparation wizards also provide information about the state of your IT environment. The wizards run over a 100 environment checks and provide data and documentation links to address any issues found.

* **Preparation Wizard**. Run the Preparation Wizard to scan your network environment and identify issues that you need to correct to be able to deploy Windows EBS.
* **Planning Wizard**. After you complete the Preparation Wizard, run the Planning Wizard to collect information about the network settings that you will need to install Windows EBS.

You must run the Preparation Wizard and the Planning Wizard before you install Windows EBS. When you complete the Planning Wizard, you save and print a custom report that contains data to use during the Windows EBS software installation.

You may need to perform additional preparation and planning tasks before you begin the Windows EBS software installation. The Preparation Wizard may require that you make specific changes to your environment to prepare it to install Windows EBS. You should also perform planning tasks that are not included in the Planning Wizard, including evaluating your options in Windows EBS for the DHCP Server service, the Domain Name System (DNS) role, and data storage.

After you complete the preparation and planning steps, you are ready to install the Windows EBS software.

Core Infrastructure Optimization Overview

# Audience

This document is designed for IT professionals and Value-added Partners who are responsible for planning, deploying, and operating IT systems for midsize business and who want to implement the technology and procedural concepts of the Core Infrastructure Optimization (Core IO) Model in part by deploying Microsoft Essential Business Server (EBS). Before explaining how EBS satisfies Core IO capabilities and attributes, a brief review of the model is provided.

# 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 IO) | Identity and Access Management |
| Desktop, Device and Server Management |
| Data Protection and Recovery |
| Security and Networking |
| IT and Security Process |
| Application Platform Infrastructure Optimization Model (AP IO) | User Experience |
| SOA and Business Process |
| Data Management |
| Development |
| Business Intelligence |
| Business Productivity Infrastructure Optimization Model (BP IO) | 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 document.

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.

# Core Infrastructure Optimization Capabilities

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

## Identity and Access Management

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

## Desktop, Device and Server Management

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

## Data Protection and Recovery

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

## Security and Networking

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

## IT and Security Process

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

# 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, "We Fight Fires"

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 software updates, software deployments, and services are provided manually.

## Optimization Level 2: Standardized, "We're Gaining Control"

The Standardized infrastructure introduces controls through the use of standards and policies to manage desktops and servers; to control the way computers or devices 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 software updates, 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, "We Enable Business"

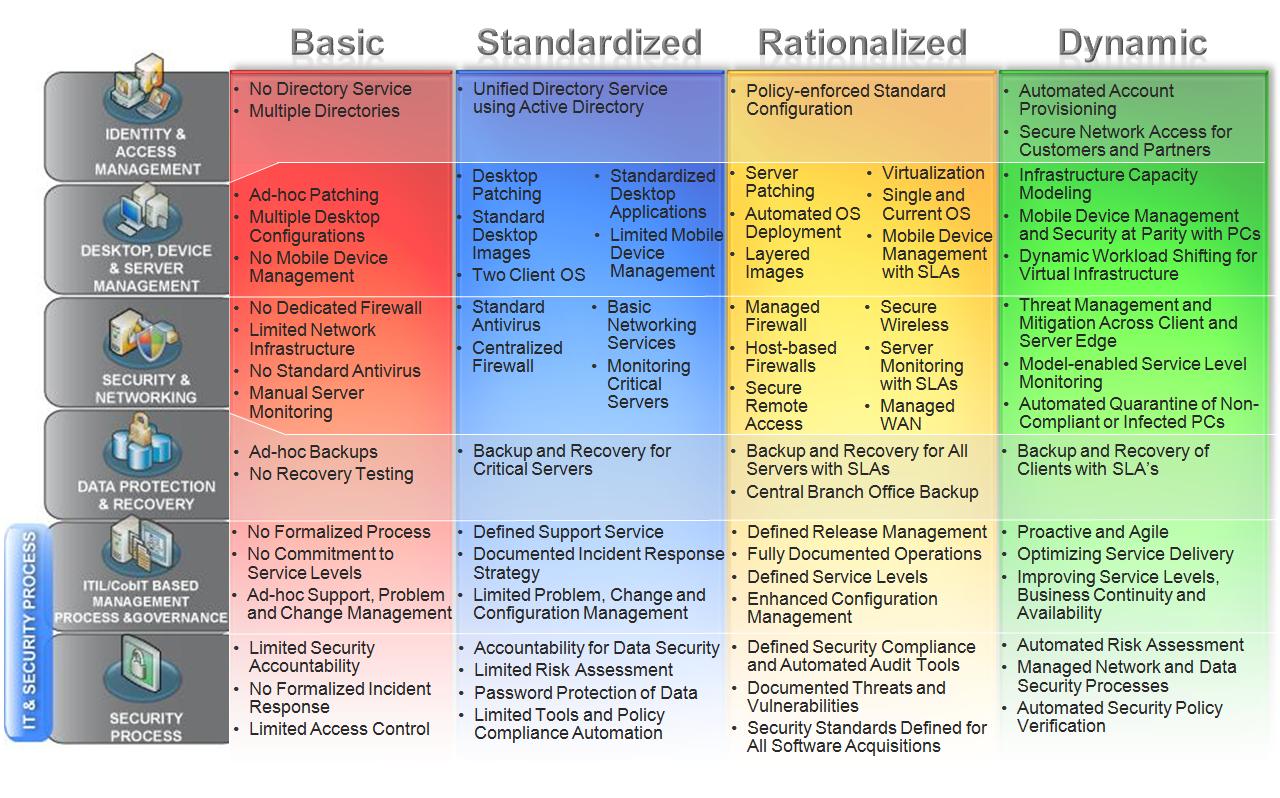
The Rationalized infrastructure is where the costs involved in managing desktops and servers are at their lowest and processes and policies have been optimized to begin playing a large role in supporting and expanding the business. Security is very proactive and responding to threats and challenges is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

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 update management and compliance with established security policies allows the Dynamic infrastructure organization to automate processes, thus helping improve reliability, lower costs, and increase service levels.

Core Infrastructure Optimization Capability Overview

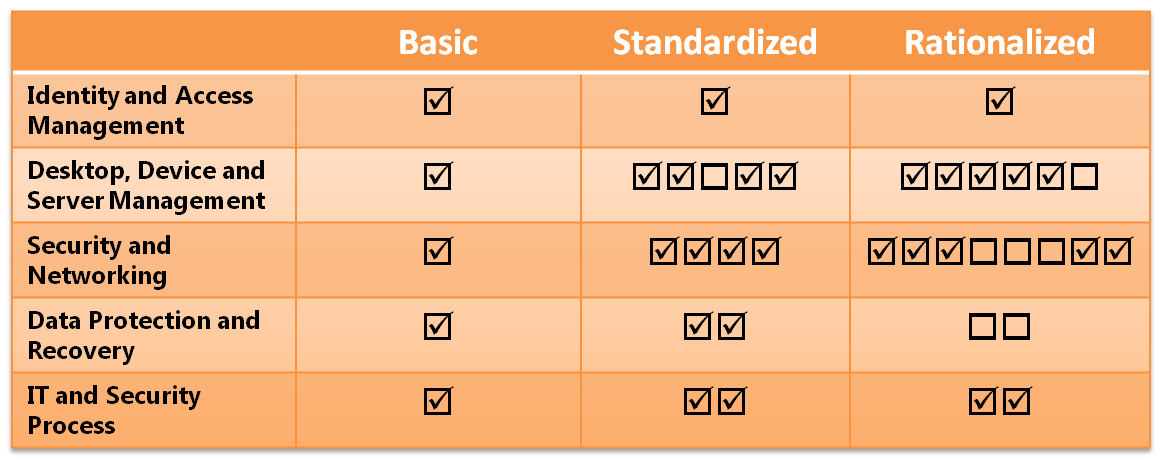
The following image lists the basic requirements for each capability to advance through the optimization levels.



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

How Essential Business Server Implements Core IO

Microsoft Essential Business Server helps you achieve a Rationalized core infrastructure by completing a standard installation. Each row in the Standardized and Rationalized columns are divided by the five Core IO capabilities. Within the column, each box represents an attribute of the capability. A checked box indicates that EBS meets or exceeds that attribute in a standard installation. An unchecked box indicates that additional configuration, products, or processes may be required to satisfy the attribute.



Network and system administrators use the Core IO maturity model to assess the effectiveness and completeness of their IT infrastructure. Each of the five capabilities of the Core IO model has several attributes. Each attribute has zero or more characteristics to evaluate against the current infrastructure. Each attribute is also part of the Standardized or Rationalized level of the Core IO maturity model.

This remainder of this document is organized around the five Microsoft Core IO capabilities. For each capability, a summary table displays if and how Essential Business Server meets or exceeds the attributes of the capability. If EBS meets the attributes by a standard installation or by external processes, a check mark appears in the appropriate column. If the attribute is not met by a standard installation, an empty box appears. The empty boxes represent gaps that remain after completing a standard installation of EBS. Please refer to the “Step By Step Guide to a Rationalized Essential Business Server Implementation” white paper to learn how to configure EBS to close all gaps documented here.

## Identity and Access Management

✓ The Core IO level is met by EBS standard installation or by processes outside the installation.

🞎 To meet the Core IO level additional software or configuration beyond a standard installation is required.

| Identity and Access Management | | | |
| --- | --- | --- | --- |
| **Standardized** | | **Rationalized** | |
| ✓ | Implemented Active Directory directory service for authentication of 80 percent or more of connected users | ✓ | Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops |

### Identity and Access Management Checkpoint Questions

|  | **Question** | **EBS Feature** | **Response** |
| --- | --- | --- | --- |
|  | Does this organization use Active Directory for authenticating 80% or more of their users? | Windows Server 2008 Active Directory | Yes. During the Windows Essential Business Server (EBS) installation, the Security and Messaging servers are automatically joined to the domain. Adding 80% or more of the users and clients to Active Directory satisfies this requirement. |
|  | Does this organization have a directory based tool to centrally define and enforce configuration standards and security on 80% or more of their desktops (for example Group Policy)? | SCE Feature Configuration Wizard, Windows Active Directory | Yes. Use the System Center Essentials Feature Configuration Wizard to create Group Policy Objects (GPOs) to manage your network.  Use the Group Policy Management Console (GPMC) to enforce user and computer configuration standards and security. |
|  | Does this organization have a central tool to automate user account provisioning (for example creating new accounts, changing passwords, synchronizing permissions, enabling access to business applications) across 80% or more of their heterogeneous systems? | EBS New User Account Wizard | Yes. This attribute is met using the Windows EBS New User Account Wizard, which enables templates for consistent creation of:   * User accounts in Active Directory directory services, assignment to DL’s and security groups * Mailboxes on Exchange * My Documents Redirection settings * License allocation |
|  | Does this organization have a solution for user identity validation and data protection – if lost – for their Mobile devices? | Exchange Server 2007 | Yes. Windows EBS protects mobile data from unauthorized access when devices are lost by wiping data remotely and locally. A new feature of Exchange 2007 enables users who lose their devices to wipe their data immediately using a Web browser and without IT assistance. This increases data protection by reducing the time between loss of the device and removal of the data.  You can also create Device Security policies on Exchange Server and use Exchange ActiveSync to deliver them to mobile devices to enforce security policies. Polices may include forcing the device to use a Personal Identification Number (PIN) to lock the device, specify the password strength and attributes, when to perform a local wipe based on number of failed attempts to access it, and the ability to exempt devices from policy enforcement. |
|  | Does this organization require a secured and guaranteed way to verify secure communications between their corporate network and mobile devices (certificates)? | Exchange Server 2007 | Yes. Exchange Server 2007, included with Windows Essential Business Server, utilizes SSL to secure communication between the corporate network and mobile devices.  Exchange 2007 Server supports certificate-based communication for both message transport via SSL and for message authentication. |

## Desktop, Device, and Server Management - Standardized

✓ The Core IO level is met by EBS standard installation or by processes outside the installation.

🞎 To meet the Core IO level additional software or configuration beyond a standard installation is required.

| Desktop, Device, and Server Management | | | |
| --- | --- | --- | --- |
| **Standardized** | | **Rationalized** | |
| ✓ | Automated software update distribution covering 80 percent or more of your desktops | ✓ | Tests and certifies application compatibility on 80 percent of new or updated applications before deploying them to desktops |
| ✓ | A defined set of standard, basic images for 80 percent or more of your desktops and portable computers | ✓ | Software management solution for 80 percent or more of your servers |
| 🞎 | A centralized solution to track, manage, and upgrade your mobile devices | ✓ | Secured and guaranteed way to verify secure communications between your corporate network and mobile devices |
| ✓ | A solution for user identity validation and data protection, if lost, for your mobile devices | ✓ | Access provided to Web applications via WAP or HTTP for mobile devices |
| ✓ | A maximum of two operating system versions on 80 percent of your desktops | ✓ | Planning for server consolidation with virtualization |
|  |  | 🞎 | Implemented a layered-image strategy for managing your desktop images |

### Desktop, Device, and Server Management Checkpoint Questions

| **Question** | **EBS Feature** | **Response** |
| --- | --- | --- |
| Does this organization have administrator-controlled automated software distribution covering 80% or more of their desktops? | EBS Administrator Console, System Center Essentials (SCE) | Yes. Admin console to monitor status. Admin console notifies of update status. Use System Center Essentials 2007 (SCE) to view, download, and deploy software updates required by operating systems and other software on managed computers.  SCE uses computer groups to deploy software updates. Either use the predefined computer groups or define your own Computer groups for update deployment. You can also configure update management to automatically approve specific types of updates for selected computer groups as those updates are downloaded. Deployment of those updates starts immediately with no administrative intervention. |
| Does this organization have an automated tracking of hardware and software assets of 80% or more of their desktops? | SCE Discovery Wizard | Yes. Use SCE to inventory network devices using the System Center Essentials Discovery Wizard. Both hardware and software inventories are maintained and viewable in System Center Essentials. Inventory information includes: operating system, including service packs, manufacturer, memory, disk space usage, installed software, and CPU performance. |
| Does this organization have a defined set of standard basic images for 80% or more of their desktops (including portable computers)? | Windows deployment Services (WDS) | Yes. Use Windows Deployment Services (WDS) to create, manage, and deploy images to desktops. |
| Does this organization have 80% or more of their desktops running Windows XP SP2 or newer as their primary OS? | SCE | Yes. Use System Center Essentials to inventory and confirm that more than 80% of your desktops are running Windows XP SP2 or newer as their primary operating system. |
| Does this organization have 80% or more of their desktops running Office 2003 or newer? | SCE | Yes. Use System Center Essentials to inventory and confirm that more than 80% of your desktops are running Office 2003 or newer. |
| Does this organization have formalized application compatibility testing and packaging to certify and automatically deploy 80% or more of their application installations? | SCE New Software Package Wizard | Yes. Use the System Center Essentials New Software Package Wizard to create a software package for deployment. A package may be approved for one or more computer groups per organization policy. Deployments may also be scheduled for a specific date and time. |
| Does this organization use virtualization within their test environment? | Windows Server 2008 Hvper-V Role | No. Add the Hyper-V role to EBS Premium and create virtual machines for use within the test environment. |
| Does your organization host desktops or applications through traditional server based computing (like Terminal Services) in the data center that users can access from their client devices? | Terminal Services, Remote Web Workplace | Yes. Add the Terminal Services role to Windows EBS to host desktop applications or use Remote Web Workplace to connect to a desktop computer. |
| Does this organization have administrator-controlled software management solution for 80% or more of their servers? | EBS Administration Console | Yes. Admin console to inventory hardware and software assets, scan servers for updates, and distribute software updates for Windows and third-party software. |
| Does this organization have a capacity modeling process solution when designing, expanding or optimizing key IT services (such as e-mail)? | EBS Infrastructure | Yes. Because Windows Essential Business Server 2008 is specifically designed for midsize businesses, much of the capacity modeling has been done for you. |
| Does this organization have a centralized solution to track, manage and upgrade their mobile devices? | Exchange Server 2007 ActiveSync | Yes. Use Exchange Server 2007 to track and manage Exchange ActiveSync users and devices. Exchange Server maintains a list of devices associated with users, enables detailed device monitoring and error reporting. |
| Does this organization have a centralized solution to track, manage and upgrade their connected non-PC devices (client devices)? | SCE | Yes. Use System Center Essentials to centralize the tracking of connected, SNMP-enabled non-PC devices such as routers, print servers, and computers running operating systems other than Windows. SCE supports network devices that are SNMP version 1 or version 2 enabled. You can use management packs from device manufacturers that contain device-specific rules and tasks. You can also configure rules and monitors using SNMP GET and SET to collect data and run tasks such as resetting the device.  SCE deploys software and updates (both Microsoft and non-Microsoft updates) to managed computers.SCE does not, however, update non-pc devices. |
| Does this organization offer access to Web applications via WAP or HTTP for Mobile Devices? | ForeFront Threat Management Gateway (TMG) | Yes. Publish via ForeFront TMG Medium Business Edition. |
| Does this organization have an automated software management solution for their mobile devices? | Exchange Server 2007 ActiveSync | Yes. Windows EBS provides automated software management using Exchange Server 2007 and ActiveSync. |
| Does this organization have an automated software management solution for their connected non-PC devices (client devices)? | SCE, device manufacturer management packs | Yes. SCE You can use management packs from device manufacturers that contain device-specific rules and tasks. You can also configure rules and monitors using SNMP GET and SET to collect data and run tasks such as resetting the device. |
| Does this organization have monitoring for 80% or more of their critical servers for ensuring consistent and reliable user experiences (for example ensuring that e-mail is always available)? | EBS Administration Console – Health Tab | Yes. Windows EBS provides a single-console view of all critical business functions. Use the Windows EBS Administration console to view server (and client) health across the organization. |
| Admin console screenshot.png | | |
| Does this organization have SLA defined and centralized monitoring solution for 80% or more of their servers with availability reporting capabilities? | SCE | Yes. Although the definition of an SLA is specific to an organization, EBS provides a centralized monitoring solution to demonstrate whether or not the SLA is being met.  During Windows EBS installation, the Management Server, Security Server, and Messaging Server are automatically configured to be managed by System Center Essentials. Once an SLA is defined, use System Center Essentials reporting capability to generate an Availability report from the Microsoft Generic Report Library. Filter the report by Warning, Monitoring unavailable, Planned Maintenance, Unplanned Maintenance, Monitor disabled, and Unmonitored. |
| Does this organization use agentless failure monitoring for client systems (PCs, portable computers, embedded) to collect, aggregate, and report application and operating system failures? | SCE Agentless Exception Monitoring | Yes. System Center Essentials provides Agentless Exception Monitoring, which is the process by which managed computers send error reports to a specified location on the System Center Essentials Management Server when an application error such as a program failure occurs on the managed computer. The error reports can help you understand which applications in your environment are having problems.  You can activate or deactivate Agentless Exception Monitoring in the Essentials 2007 Feature Configuration Wizard. |
| Does this organization have health and availability monitoring for client systems (PCs, portable computers, embedded) for ensuring both optimal uptime and a consistent and reliable user experience? | SCE Group Summary Report | Yes. Windows EBS provides a single-console view of all critical business functions.  Use System Center Essentials to create a Group Summary report of servers. The SCE report displays operating system version and service pack, model name, drives grouped by space usage, list of installed software, health status (alerts, updates, software, and contact). |
| Does this organization have configuration monitoring for their client systems for ensuring optimal uptime and compliance to policy? | SCE | Yes. System Center Essentials provides numerous monitoring and reporting options to ensure that client systems are in compliance with policy. Use SCE to monitor Office configuration compliance, client operating system compliance, server compliance, and any SNMP-enabled network device. |
| Does this organization monitor and report server configuration compliance against baselines or regulatory requirements? | SCE Group Summary Report | Yes. Windows EBS provides a single-console view of all critical business functions.  Use System Center Essentials to create a Group Summary report of servers. The SCE report displays operating system version and service pack, model name, drives grouped by space usage, list of installed software, health status (alerts, updates, software, and contact). |

## Security and Networking

✓ The Core IO level is met by EBS standard installation or by processes outside the installation.

🞎 To meet the Core IO level additional software or configuration beyond a standard installation is required.

|  |  |  |  |
| --- | --- | --- | --- |
| Security and Networking | | | |
| **Standardized** | | **Rationalized** | |
| ✓ | Antivirus software (with automated signature updating) running on 80 percent or more your desktops | ✓ | Policy-managed firewall on 80 percent or more of your servers and desktops |
| ✓ | Firewall (not per desktop) for your organization protecting 80 percent or more of your systems | ✓ | Secure remote access to internal resources and line-of-business (LOB) applications beyond e-mail (that is, VPN or Terminal Services) |
| ✓ | Internal servers for basic networking services (DNS, DHCP, WINS) | ✓ | Secured and guaranteed way to verify communication between critical servers, such as domain controllers and e-mail servers |
| ✓ | Monitoring for 80 percent or more of your critical servers to ensure a consistent and reliable user experience | 🞎 | Monitoring and service level reporting for 80 percent or more of your servers to ensure a consistent and reliable user experience |
|  |  | 🞎 | Providing a secured communication mechanism for presence |
|  |  | 🞎 | Deployed a secure wireless network using Active Directory and IAS/RADIUS for authentication and authorization |
|  |  | ✓ | Centrally managed certificate services infrastructure (PKI) |
|  |  | ✓ | Proactively managing bandwidth to branch offices |

### Security and Networking Checkpoint Questions

| **Question** | **EBS Feature** | **Response** |
| --- | --- | --- |
| Does this organization have Antivirus software (with automated signature updating) running on 80% or more their desktops? | Forefront Threat Management Gateway (TMG) | Yes. Windows EBS provides automated signature updating using an optional Web antivirus, antimalware subscription-based service with Forefront Threat Management Gateway Medium Business Edition (TMG MBE). |
| Does this organization have Antivirus, Antispyware (with automated signature updating) for the majority of their Non-PC devices? | None | No. |
| Does this organization have a central, policy managed, firewall enabled on the majority of servers? | Forefront Threat Management Gateway Medium Business Edition (TMG MBE) | Yes. A standard EBS deployment satisfies this question. EBS includes Threat Management Gateway Medium Business Edition (TMG MBE), a critical security component and integrated edge security gateway that helps provide protection from multiple Internet-based threats. TMG MBE also provides secure connectivity, and simplified management for midsize businesses. |
| Does this organization have a centralized perimeter firewall (not per desktop) for their enterprise protecting 80% or more of their systems? | Microsoft Forefront Technology, Windows Firewall with Advanced Security and IPSec | Yes. Windows EBS provides perimeter protection using the Forefront family of products and can also integrate into an existing firewall solution.  Windows Firewall with Advanced Security supports separate profiles for when computers are members of a domain, or connected to a private or public network. It also supports the creation of rules for enforcing server and domain isolation policies. Windows Firewall with Advanced Security supports more detailed rules than previous versions of Windows Firewall, including users and groups in Active Directory, source and destination Internet Protocol (IP) addresses, IP port number, ICMP settings, IPsec settings, specific types of interfaces, services, and more. |
| Does this organization have internal servers for basic network services (DNS, DHCP)? | Windows Server 2008 | Yes. Windows EBS provides internal servers for basic network services. Best practice for most EBS deployments is for the Management server to be the only DHCP server in your environment. If the Management server is the only server in your environment management tasks are reduced, monitoring is more straightforward and security is easier to manage. |
| Does this organization have integrated threat management and mitigation across client, server edge? | Microsoft Forefront Edge Technology | Yes, EBS uses the Forefront Threat Management Gateway MBE, Forefront Server security and Edge Security to mitigate threats across the organization. |
| Does this organization provide a secured communication mechanism for presence? | No | Yes. Use Live Communications Server 2005 or Office Communication Server 2007 to provide a secured communication mechanism for presence. |
| Does this organization have a centrally managed certificate services infrastructure (PKI)? | Active Directory Certificate Services, Windows Server 2008, Enterprise PKI Snap-in | Yes. In addition to the Enterprise PKI snap-in provided by Windows Server 2008 to view, monitor, and manage the status of all certification authorities (CA), Windows EBS installs the Active Directory Certificate Services server role on the Management Server. This creates a single-tier enterprise public key infrastructure (PKI) hierarchy with a certification authority that is specific to the Windows EBS domain. This private certification authority issues self-signed certificates that are used by default by Forefront TMG for publishing secure Web sites such as Outlook Web Access and Remote Web Workplace. |

## Data Protection and Recovery

✓ The Core IO level is met by EBS standard installation or by processes outside the installation.

🞎 To meet the Core IO level additional software or configuration beyond a standard installation is required.

|  |  |  |  |
| --- | --- | --- | --- |
| Data Protection and Recovery | | | |
| **Standardized** | | **Rationalized** | |
| ✓ | Backup and restore solution for 80 percent or more of your business-critical servers | 🞎 | Centrally managing data backup for your branch offices |
| ✓ | Centrally managing data backup for your branch offices | 🞎 | Service level agreement (SLA) for system backup and restore, and defined recovery times for 80 percent of your servers |

### Data Protection and Recovery Checkpoint Questions

|  | **Question** | **EBS Feature** | **Response** |
| --- | --- | --- | --- |
|  | Does this organization have backup and restore with SLA-defined recovery times for 80% or more of their servers? | Windows Server Backup | Use Native EBS (Windows Server Backup) for component-level backup. |
|  | Does this organization have a defined and managed backup and restore solution for 80% or more of their business critical servers? | None | No native EBS solution. |
|  | Does this organization centrally manage branch office data backup? | None | No native EBS solution, use Microsoft Data Protection Manager 2007 |
|  | Does this organization use virtualization as a tool for enabling backup / disaster recovery protection of servers and applications? | None | No native EBS solution. |
|  | Does this organization use clustering or similar technology to achieve defined availability targets of applications and services? | None | Not supported by EBS. |

## IT and Security Process

As the name indicates, IT and Security Process is process, rather than feature oriented, however, tools and product features can alleviate much of the burden of assessing, monitoring, and enforcing IT Security policies. Essential Business Server does not define processes for you, but provides monitoring tools, integrated consoles, alert mechanisms and more to enable the successful implementation of the attributes of the IT and Security Process capability.

✓ The Core IO level is met by EBS standard installation or by processes outside the installation.

🞎 To meet the Core IO level additional software or configuration beyond a standard installation is required.

|  |  |  |  |
| --- | --- | --- | --- |
| IT and Security Process | | | |
| **Standardized** | | **Rationalized** | |
| ✓ | Risk assessment methodology and incident response plan, consistent security policy compliance, and evaluation and testing of all acquired software | ✓ | Established security processes for two-factor user authentication, standard security review for new software acquisitions, and data classification |
| ✓ | A defined process for problem, incident, service, configuration, and change management | ✓ | Implemented best practices for operating, optimizing, and change processes in your IT organization |

### IT and Security Process Checkpoint Questions

|  | **Question** | **EBS Feature** | **Response** |
| --- | --- | --- | --- |
|  | Does this organization have an individual who is accountable for information security and who defines security processes, risk management processes and enforcement vehicles for the organization? | Essential Business Server tools, templates, and features | This individual, once identified, is free to define IT and Security Processes to meet specific business needs and objectives and then use Essential Business Server tools, templates, and features to implement the definition. |
|  | Does this organization have a formalized information security risk management process, including conducting security risk assessments (self-assessment or 3rd-party assessment) and corresponding mitigation at appropriate intervals? | Microsoft Security Assessment Tool (MSAT), Microsoft Baseline Security Analyzer | The Microsoft Security Assessment Tool (MSAT) is a risk-assessment application designed to provide you with information and recommendations about best practices for security within your information technology (IT) infrastructure. This application is designed to help organizations with fewer than 1,000 employees better understand potential security issues. It will help identify personnel, processes, resources, and technologies that are designed to promote good security planning and risk mitigation practices within your organization.  The Microsoft Baseline Security Analyzer provides a streamlined method of identifying common security misconfigurations. |
|  | Does this organization have a formalized incident management process? | Windows Server 2008, SCE, Administrator console | EBS helps provide visibility into incident response processes and also provides tools to enforce and audit actions taken in response to an incident. Assigning actions and alerts to system conditions such as services that stop unexpectedly helps reduce response time and increase accountability for proper action within the IT staff. |
|  | Does the incident response process include a defined root cause analysis process? | Windows Server 2008, component logging and auditing | EBS provides detailed, customizable auditing for systems and components to aid in identifying and analyzing the root cause of an incident. |
|  | Does this organization have a process to manage the identity of users, devices or services? | New User Account Wizard, SCE, Group Policy Preferences | The identity management process for users, devices, and services is supported by a various features and tools available within EBS. Some of which include the New Account Wizard for consistent creation and management of users, SCE to identify and manage network devices, and Group Policy Preferences for managing server services. |
|  | Does this organization have a process to manage antivirus controls? | Forefront Server Security, Forefront Client Security (optional add-on) | Use Forefront Server Security and Forefront Client Security features to implement your organizations’ process to manage antivirus and malware controls. Antivirus policies and distribution is integrated with Active Directory and enables you to apply your policies to OUs or other Active Directory objects. This provides a greater level of control to implement your organization’s specific processes and policy. |
|  | Does this organization have a process to deploy security updates to all network-connected IT assets? | SCE | A security update deployment process can be easily executed using SCE. SCE can deploy both msi and non-msi programs. SCE also incorporates an approval process. |
|  | Does this organization have a process to verify security policy compliance of all network-connected devices? | SCE | Use SCE to view and enforce software compliance. Use Essentials 2007 choose to automatically deploy critical updates or have them be subject for approval, and track compliance across your network. Deployments may also be done in real in time. |
|  | Does this organization follow a security review process for software acquisition (commercially-available, custom & internally-developed)? | SCE | After your software acquisition process is defined and implemented, use SCE’s detailed inventory features and reports to ensure that no unauthorized or rogue software applications are appearing on your network. |
|  | Does this organization have a process to classify data and apply appropriate data security controls? |  | After data has been properly classified, use Windows Server 2008 access control features with Active Directory to apply appropriate data controls to protect your data. |
|  | Does this organization have formalized processes for IT support services, problem management, change management and configuration management? | N/A | No. |
|  | Does this organization have formalized processes for system administration, service monitoring and network administration? | SCE, Admin Console | The Administration Console can be used to monitor the status of the key services and components that determine whether users can log on to the domain, access the Internet, and send and receive e-mail. |

# Appendix A – Detailed Description of Capabilities

## Identity and Access Management

### Standardized

Implemented Active Directory directory service for authentication of 80 percent or more of connected users

### Rationalized

Implemented a directory-based tool to centrally administer configurations and security on 80 percent or more of your desktops

Attributes:

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

## Desktop, Device, and Server Management

### Standardized

Automated software distribution covering 80 percent or more of your desktops.

Attributes:

* Implemented process and tools to inventory hardware and software assets.
* Implemented process and tools to scan client computers for software updates.
* Established a process to automatically identify available software updates.
* Established standard testing for every software update.
* Implemented update distribution software.

A defined set of standard, basic images for 80 percent or more of your desktops and portable computers

Attributes:

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

A centralized solution to track, manage, and upgrade your mobile devices

Attributes:

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

A solution for user identity validation and data protection, if lost, for your mobile devices

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

A maximum of two operating system versions on 80 percent of your desktops

Attributes:

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

### Rationalized

Tests and certifies application compatibility on 80 percent of new or updated applications before deploying them to desktops

Attributes:

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

Software management solution for 80 percent or more of your servers

Attributes:

* Implemented process and tools to inventory hardware and software assets.
* Implemented process and tools to scan servers for software updates.
* Established a process to automatically identify available software updates.
* Established standard testing for every software update.
* Implemented update distribution software.

Secured and guaranteed way to verify secure communications between your corporate network and mobile devices

Attributes:

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

Access provided to Web applications via WAP or HTTP for mobile devices

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

Planning for server consolidation with virtualization

Attributes:

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

Implemented a layered-image strategy for managing your desktop images

Attributes:

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

## Security and Networking

### Standardized

Antivirus software (with automated signature updating) running on 80 percent or more your desktops

Attributes:

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

Firewall (not per desktop) for your organization protecting 80 percent or more of your systems

Internal servers for basic networking services (DNS, DHCP, WINS)

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

### Rationalized

Monitoring for 80 percent or more of your critical servers to ensure a consistent and reliable user experience

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

Policy-managed firewall on 80 percent or more of your servers and desktops

Attributes:

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

Secure remote access to internal resources and line-of-business (LOB) applications beyond e-mail (that is, VPN or Terminal Services)

Attributes:

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

Secured and guaranteed way to verify communication between critical servers, such as domain controllers and e-mail servers

Attributes:

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

Monitoring and service level reporting for 80 percent or more of your servers to ensure a consistent and reliable user experience

Attributes:

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

Providing a secured communication mechanism for presence

Attributes:

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

Deployed a secure wireless network using Active Directory and IAS/RADIUS for authentication and authorization

Attributes:

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

Centrally managed certificate services infrastructure (PKI)

Attributes:

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

Proactively managing bandwidth to branch offices

Attributes:

* Identified and documented branch office topology.
* Created requirement specification based on the needs of all branch office types.
* Created a plan and architecture for branch office service consolidation and identified performance thresholds for reexamination of branch office WAN requirements.
* Implemented plan to optimize branch office services against WAN link limitations.

## Data Protection and Recovery

### Standardized

Backup and restore solution for 80 percent or more of your business-critical servers

Attributes:

* Created a data backup plan and a recovery plan for eighty percent or more of your critical servers.
* Used drills to test your plans.

### Rationalized

Centrally managing data backup for your branch offices

Attributes:

* Created a centralized data backup plan and a recovery plan for branch offices in your organization.
* Implemented a backup and recovery plan for centralized control of backup and recovery operations, either via network-centralized tools or operational guidelines for local backup and recovery, with defined service levels.

Service level agreement (SLA) for system backup and restore, and defined recovery times for 80 percent of your servers

Attributes:

* Created a data backup plan and a recovery plan for 80 percent or more of all servers in your organization.
* Used drills to test your plans and validate defined recovery times.

## IT and Security Process

### Standardized

Risk assessment methodology and incident response plan, consistent security policy compliance, and evaluation and testing of all acquired software

Attributes:

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

A defined process for problem, incident, service, configuration, and change management

Attributes:

* Implemented Problem Management techniques.
* Implement Incident Management techniques.
* Improved end-user support services.
* Implemented Change Management best practices.

### Rationalized

Established security processes for two-factor user authentication, standard security review for new software acquisitions, and data classification

Attributes:

* Developed and implemented two-factor identity and access management policies.
* Developed a process to manage security requirement testing on all acquired or developed software.
* Established a standard and repeatable procedure for classifying sensitive data.

Implemented best practices for operating, optimizing, and change processes in your IT organization

Attributes:

* Implemented service level management across IT operations.
* Implemented best practice release management.
* Optimized network and system administration processes.
* Implemented best practice job scheduling.

# Appendix B – Additional resources

For more information about Essential Business Server, visit:

http://www.microsoft.com/ebs

For more information about Windows Essential Server Solutions, visit:

http://www.microsoft.com/wess

For more information about Exchange Server 2007, visit:

http://www.microsoft.com/exchange

For more information about SQL Server 2005, visit:

http://www.microsoft.com/sqlserver/2005

For more information about SQL Server 2008, visit:

http://www.microsoft.com/sqlserver/2008

For more information about Microsoft Core Infrastructure Optimization, visit:

http://www.microsoft.com/infrastructure/about/overview.mspx

For more information about Microsoft Forefront Security Products for Business, visit:

http://www.microsoft.com/forefront

For more information about Forefront Threat Management Gateway Medium Business Edition, visit:

http://www.microsoft.com/forefront/edgesecurity/isaserver/en/us/threat-management-gateway-mbe.aspx

# Appendix C – Assumptions

### Security and Networking Assumptions:

* That TMG is deployed to more than 80% of the servers in the organization.
* Antivirus software (with automated signature updating) running on 80 percent or more your desktops
* Your organization has a central, policy managed, firewall enabled on the majority of its servers.

### Desktop, Device, and Server Management Assumptions:

* A maximum of two operating system versions are installed on 80 percent of your desktops in your organization.