the CENTER for INTERNET SECURITY

Security Configuration Benchmark For

Microsoft Office SharePoint Server 2007

Version 1.0.0

December 5th, 2011

http://cisecurity.org

feedback@cisecurity.org

Background.

CIS provides benchmarks, scoring tools, software, data, information, suggestions, ideas, and other services and materials from the CIS website or elsewhere ("**Products**") as a public service to Internet users worldwide. Recommendations contained in the Products ("**Recommendations**") result from a consensus-building process that involves many security experts and are generally generic in nature. The Recommendations are intended to provide helpful information to organizations attempting to evaluate or improve the security of their networks, systems and devices. Proper use of the Recommendations requires careful analysis and adaptation to specific user requirements. The Recommendations are not in any way intended to be a "quick fix" for anyone's information security needs.

No representations, warranties and covenants.

CIS makes no representations, warranties or covenants whatsoever as to (i) the positive or negative effect of the Products or the Recommendations on the operation or the security of any particular network, computer system, network device, software, hardware, or any component of any of the foregoing or (ii) the accuracy, reliability, timeliness or completeness of any Product or Recommendation. CIS is providing the Products and the Recommendations "as is" and "as available" without representations, warranties or covenants of any kind.

User agreements.

By using the Products and/or the Recommendations, I and/or my organization ("**we**") agree and acknowledge that:

No network, system, device, hardware, software or component can be made fully secure;
We are using the Products and the Recommendations solely at our own risk;

We are not compensating CIS to assume any liabilities associated with our use of the Products or the Recommendations, even risks that result from CIS's negligence or failure to perform;

We have the sole responsibility to evaluate the risks and benefits of the Products and Recommendations to us and to adapt the Products and the Recommendations to our particular circumstances and requirements;

Neither CIS, nor any CIS Party (defined below) has any responsibility to make any corrections, updates, upgrades or bug fixes or to notify us if it chooses at it sole option to do so; and

Neither CIS nor any CIS Party has or will have any liability to us whatsoever (whether based in contract, tort, strict liability or otherwise) for any direct, indirect, incidental, consequential, or special damages (including without limitation loss of profits, loss of sales, loss of or damage to reputation, loss of customers, loss of software, data, information or emails, loss of privacy, loss of use of any computer or other equipment, business interruption, wasted management or other staff resources or claims of any kind against us from third parties) arising out of or in any way connected with our use of or our inability to use any of the Products or Recommendations (even if CIS has been advised of the possibility of such damages), including without limitation any liability associated with infringement of intellectual property, defects, bugs, errors, omissions, viruses, worms, backdoors, Trojan horses or other harmful items.

Grant of limited rights.

CIS hereby grants each user the following rights, but only so long as the user complies with all of the terms of these Agreed Terms of Use:

Except to the extent that we may have received additional authorization pursuant to a written agreement with CIS, each user may download, install and use each of the Products on a single computer;

Each user may print one or more copies of any Product or any component of a Product that is in a .txt, .pdf, .doc, .mcw, or .rtf format, provided that all such copies are printed in full and are kept intact, including without limitation the text of this Agreed Terms of Use in its entirety.

Retention of intellectual property rights; limitations on distribution.

The Products are protected by copyright and other intellectual property laws and by international treaties. We acknowledge and agree that we are not acquiring title to any intellectual property rights in the Products and that full title and all ownership rights to the Products will remain the exclusive property of CIS or CIS Parties. CIS reserves all rights not expressly granted to users in the preceding section entitled "Grant of limited rights." Subject to the paragraph entitled "Special Rules" (which includes a waiver, granted to some classes of CIS Members, of certain limitations in this paragraph), and except as we may have otherwise agreed in a written agreement with CIS, we agree that we will not (i) decompile, disassemble, reverse engineer, or otherwise attempt to derive the source code for any software Product that is not already in the form of source code; (ii) distribute, redistribute, encumber, sell, rent, lease, lend, sublicense, or otherwise transfer or exploit rights to any Product or any component of a Product; (iii) post any Product or any component of a Product on any website, bulletin board, ftp server, newsgroup, or other similar mechanism or device, without regard to whether such mechanism or device is internal or external, (iv) remove or alter trademark, logo, copyright or other proprietary notices, legends, symbols or labels in any Product or any component of a Product; (v) remove these Agreed Terms of Use from, or alter these Agreed Terms of Use as they appear in, any Product or any component of a Product; (vi) use any Product or any component of a Product with any derivative works based directly on a Product or any component of a Product; (vii) use any Product or any component of a Product with other products or applications that are directly and specifically dependent on such Product or any component for any part of their functionality, or (viii) represent or claim a particular level of compliance with a CIS Benchmark, scoring tool or other Product. We will not facilitate or otherwise aid other individuals or entities in any of the activities listed in this paragraph.

We hereby agree to indemnify, defend and hold CIS and all of its officers, directors, members, contributors, employees, authors, developers, agents, affiliates, licensors, information and service providers, software suppliers, hardware suppliers, and all other persons who aided CIS in the creation, development or maintenance of the Products or Recommendations ("**CIS Parties**") harmless from and against any and all liability, losses, costs and expenses (including attorneys' fees and court costs) incurred by CIS or any CIS Party in connection with any claim arising out of any violation by us of the preceding paragraph, including without limitation CIS's right, at our expense, to assume the exclusive defense and control of any matter subject to this indemnification, and in such case, we agree to cooperate with CIS in its defense of such claim. We further agree that all CIS Parties are third-party beneficiaries of our undertakings in these Agreed Terms of Use.

Special rules.

CIS has created and will from time to time create special rules for its members and for other persons and organizations with which CIS has a written contractual relationship. Those special rules will override and supersede these Agreed Terms of Use with respect to the users who are covered by the special rules. CIS hereby grants each CIS Security Consulting or Software Vendor Member and each CIS Organizational User Member, but only so long as such Member remains in good standing with CIS and complies with all of the terms of these Agreed Terms of Use, the right to distribute the Products and Recommendations within such Member's own organization, whether by manual or electronic means. Each such Member acknowledges and agrees that the foregoing grant is subject to the terms of such Member's membership arrangement with CIS and may, therefore, be modified or terminated by CIS at any time.

Choice of law; jurisdiction; venue.

We acknowledge and agree that these Agreed Terms of Use will be governed by and construed in accordance with the laws of the State of Maryland, that any action at law or in equity arising out of or relating to these Agreed Terms of Use shall be filed only in the courts located in the State of Maryland, that we hereby consent and submit to the personal jurisdiction of such courts for the purposes of litigating any such action. If any of these Agreed Terms of Use shall be determined to be unlawful, void, or for any reason unenforceable, then such terms shall be deemed severable and shall not affect the validity and enforceability of any remaining provisions. We acknowledge and agree that we have read these Agreed Terms of Use in their entirety, understand them and agree to be bound by them in all respects.

Table of Contents

Overview

This document, *Security Configuration Benchmark for Microsoft Office SharePoint Server 2007*, provides prescriptive guidance for establishing a secure configuration posture for Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0 (WSS) running on Microsoft Windows 2003. This guide was tested against Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0 (WSS) running on Microsoft Windows 2003. To obtain the latest version of this guide, please visit http://cisecurity.org. If you have questions, comments, or have identified ways to improve this guide, please write us at feedback@cisecurity.org.

Consensus Guidance

This benchmark was created using a consensus review process comprised of volunteer and contract subject matter experts. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS benchmark undergoes two phases of consensus review. The first phase occurs during initial benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the benchmark. This discussion occurs until consensus has been reached on benchmark recommendations. The second phase begins after the benchmark has been released to the public Internet. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in to the CIS benchmark. If you are interested in participating in the consensus review process, please send us a note to feedback@cisecurity.org.

Intended Audience

This benchmark is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Office SharePoint Server 2007 and Windows SharePoint Services 3.0 (WSS) running on Microsoft Windows 2003.

Acknowledgements

This benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

Authors

Lisa Morrison, *MITRE*
Shirley Matthews, *National Security Agency*

Editors

Kamran Alvi, *Digital Security, Inc*
Shyam Rose

Testers

Lisa Nordman, *MITRE*
Lisa Morrison, *MITRE*

Typographic Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
`Stylized Monospace font`	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
`Monospace font`	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
<italic font in brackets>	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
Italic font	Used to denote the title of a book, article, or other publication.
Note	Additional information or caveats

Configuration Levels

This section defines the configuration levels that are associated with each benchmark recommendation. Configuration levels represent increasing levels of security assurance.

Level-I Benchmark settings/actions

Level-I Benchmark recommendations are intended to:

- be practical and prudent;
- provide a clear security benefit; and
- do not negatively inhibit the utility of the technology beyond acceptable means

Level-II Benchmark settings/actions

Level-II Benchmark recommendations exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is paramount
- acts as defense in depth measure
- may negatively inhibit the utility or performance of the technology

Scoring Status

This section defines the scoring statuses used within this document. The scoring status indicates whether compliance with the given recommendation is discernible in an automated manner.

Scorable

The platform's compliance with the given recommendation can be determined via automated means.

Not Scorable

The platform's compliance with the given recommendation cannot be determined via automated means.

1. Recommendations

1.1 Accounts

This chapter provides recommendations on the setup and management of required SharePoint accounts for both single server and server farm deployments. The account names can be tailored to suit the deployment environment. For this evaluation, the SharePoint 2007 Server was installed and configured on a single server. Recommendations pertaining to accounts for server farm deployments are derived from Microsoft documents, which are referenced within this guide.

1.1.1 Verify a Least Privileged Setup Account (Level I, Not Scorable)

Description:
Create a least privileged local user account to set-up and install SharePoint Server 2007 in single server installations. The Setup User account runs setup on each server, SharePoint Products and Technologies Configuration Wizard, the `Psconfig` command-line tool, and the `Stsadm` command-line tool. The Setup User account is local and must be a member of the Administrators group.

Rationale:
Ensure that the Setup User account follows the principles of least privilege by configuring the account with only the minimum privileges needed to accomplish the tasks it is authorized to perform. Following this practice reduces the opportunity for a malicious user or process to compromise the SharePoint environment, such as other processes and files.

Audit:
Perform the following to determine if the recommended state is established:

1. Login to the SharePoint Central Administration Console.
2. Go to the Operations tab.
3. Under Security Configuration section, click on "Update farm administrator's group."
4. In the left pane, select "Site Permissions", this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. This account should be a member of the Administrators group on the local computer.

   Server Farm Standard Requirement
   a. This account should be a member of Local Administrators group on each server running the set-up.
   b. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Server Farm using SQL Authentication

a. This account should be a member of Local Administrators group on each server running the set-up.
b. This account should NOT be a member of the Administrators group on the computer running SQL Server.
c. This account should NOT be a member of `securityadmin` and `dbcreator` fixed SQL Server role.

Server Farm using Doman user Authentication

a. This account should be a member of Local Administrators group on each server running the set-up.
b. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Remediation:

Single Server Set-Up

a. Member of the Administrators group on the local computer.

Server Farm standard Requirement

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Server Farm using SQL Authentication

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.
d. This account should NOT be a member of `securityadmin` and `dbcreator` fixed SQL Server role.

Server Farm using Domain user Authentication

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Note:

- If running the `stsadm` command affects a database, this account must be a member of the `db_owner` fixed database role.
- Change the database owner (`dbo` or `db_owner`) to the Setup User account after each database has been created.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.2 Verify a Least Privileged Office SharePoint Server Search Account (Level I, Not Scorable)

Description:

Create a least privileged Office SharePoint Server Search service account for single server installations. The Office SharePoint Server Search service encrypts sensitive search configuration settings such as passwords. This service runs by default as the Local Service built-in account.

Rationale:

Any application or service residing on the SharePoint server running as the built-in account will have access to sensitive items, reducing the confidentiality of those items. To minimize the risk of sensitive information leakage, change the search service account to a non-built-in account.

Audit:

1. From the command prompt, execute the following command: `sc.exe qc osearch`.
2. Ensure `SERVICE_START_NAME` attribute is not `NT AUTHORITY\LocalService`.

Remediation:

Follow these steps to implement this recommendation:

1. Create a local account on the SharePoint Server.
2. Login to Central Administration.
3. Navigate to Operations, Topology and Services.
4. Select Services on Server.
5. Select Office SharePoint Server Search.
6. Navigate to Farm Search Service Account.
7. Select Configurable.
8. Enter the username and password of the account created in step 1.
9. Select OK.

Note:

- After the configuration database and the Central Administration content databases are created, add this account to the Users group and `WSS_Content_Application_Pools` role databases.

- After the SSP database and the SSP search database are created, add this account to the Users group and `db_owner` role.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.3 Verify a Dedicated Excel Services Unattended Service Domain Account (Level 1, Not Scorable)

Description
Create a dedicated Excel Services Unattended Service domain account for single server and server farm installations. The Excel Services Unattended Service domain account connects Excel Calculation Services uses to external data sources that require a non-Windows user name and password for authentication. The default configuration setting will not connect to non-Windows data sources without a specified account.

Rationale:
Minimizing privileges needed to perform tasks by the Excel Services Unattended Service domain account reduces the opportunity for a malicious user or process to compromise the SharePoint environment. If the built-in account is compromised, an access token can be used to manipulate other services running the same account, thereby reducing the overall confidentiality of the system. To minimize the risk of this threat, change the Excel Service account to a non-built-in account.

Audit:
1. Login to the SharePoint Central Administration Console.
2. Go to the Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions - this displays the Central Administration Permissions.
5. Note the user accounts with permissions.
6. Check and edit the permissions of the user account in the following environments:
    a. Single Server Set-Up
    b. Server Farm Standard Requirement
    c. Server Farm using SQL Authentication
    d. Server Farm using Doman user Authentication.

Remediation:
Single server Set-Up, Server Farm standard requirement, Server Farm Using SQL Authentication and Server Farm using Domain User Authentication requirement: must be a domain user account.

Additional Reference(s):
1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.4 Verify a Least Privileged Separate Domain User Account for Each Application Pool (Level 1, Not Scorable)

Description:
Create a separate domain user account for application pools in server farm installations. An application pool domain account is an identity for Web applications that reside within the application pool. A default account is automatically setup and configured for the default application pool.

Rationale:

In standard server farms, provide isolation among application pools by using a separate domain account for each application pool. Follow the principle of least privilege by creating an account that is not a member of the Administrator's group and exhibits minimum privileges needed to accomplish the tasks intended to perform. This reduces the opportunity for a malicious user or process to compromise the SharePoint environment. If one account is compromised, a malicious user only has access to data for the specific application pool's account and other accounts, processes, and files are at a lesser risk of compromise.

Audit:

1. Login to SharePoint Central Administration Console.
2. Go to Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. Check if the Network Service account is used for the default web site that is created during Setup and configuration.
   b. The account should NOT be a member of the Administrators group on any server in the farm, including the computer running SQL Server.

   Server Farm using SQL Authentication
   a. The account should NOT be a member of the Administrators group on any server in the server farm, including the computer running SQL Server.
   b. The account should NOT be a SQL Server login on the computer running SQL Server.

   Server Farm using Doman user Authentication
   a. This account should not be a member of the Administrators group on any computer in the server farm.

Remediation:

Single Server Set-Up
a. No manual configuration is necessary.
b. The Network Service account is used for the default Web site that is created during Setup and configuration.
c. Use a separate domain user account NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.

Server Farm using SQL Authentication
a. Use a separate domain user account NOT a member of the Administrators group on any server in the server farm, including the computer running SQL Server.

b. NOT a SQL Server login on the computer running SQL Server.

Server Farm using Domain User Authentication

a. Use a separate domain user account.
b. This account should not be a member of the Administrators group on any computer in the server farm.
c. This account does not require permissions to SQL Server before creating the configuration database.

Note:

- This account does not require permissions to SQL Server before creating the configuration database.
- After the Shared Services Provider (SSP) database and the SSP search database are created, add this account to the Users group and `db_owner` fixed database role.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.5 Verify a Least Privileged Office SharePoint Server Search Service Domain Account. (Level 1, Not Scorable)

Description

Create a dedicated Office SharePoint Server Search Service domain account in server farm installations. The Office SharePoint Server Search Service domain account is used as the service account for the Office SharePoint Server Search service. A single instance of this service is used by all SSPs. The account must be a domain user account and must not be a member of the Farm Administrators group.

Rationale:

Ensure that the Office SharePoint Server Search Service domain account is provided with only the minimum privileges needed to accomplish the tasks it is intended to perform. This practice adheres to the principle of least privilege by reducing the opportunity for a malicious user or process to compromise the SharePoint environment. Having unique accounts increases data protection. If one account is compromised, a malicious user will have access only to data for the compromised account.

Audit:

1. Login to SharePoint Central Administration Console.
2. Go to Operations tab.
3. Under Security Configuration section click on “Update farm administrator’s group.”
4. In the left pane select “Site Permissions” - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

Single Server Set-Up

a. Check if the account is running as the Local system account.

Server Farm Standard Requirement

a. This account should be a separate domain account.

Server Farm using SQL Authentication

a. The account should NOT be a member of the Administrators group on any server in the farm, including the computer running SQL Server.
b. The account should NOT be a SQL Server login.

Server Farm using Doman user Authentication

a. This account should not be a member of the Administrators group on any computer in the server farm.

Remediation:

Single Server Set-Up

a. This account by default runs as the Local system account.

Server Farm standard requirement

a. User is a separate domain account

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.
c. NOT a SQL Server login.

Server Farm using Domain User Authentication

a. Use a separate domain account.

Note:

- After the SSP database and the SSP search database are created, add this account to the Users group and `db_owner` role for each of these databases.
- After the configuration database and the Central Administration content databases are created, add this account to the Users group and `WSS_Content_Application_Pools` role for these databases.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.6 Verify a Least Privileged SQL Server Service Account (Level, Not Scorable)

Description:

Create a dedicated SQL Server Service domain account in server farm installations. The SQL Server prompts for this domain account during SQL Server setup which used as the service account for the following SQL Server services: `MSSQLSERVER` and `SQLSERVERAGENT`.

Rationale:
Ensure that the SQL Server Service domain account is provided with only the minimum privileges needed to accomplish the tasks it is intended to perform. This practice adheres to the principle of least privilege by reducing the opportunity for a malicious user or process to compromise the SharePoint environment. A unique account increases data protection. If one account is compromised, the malicious user will have access only to data for the account.

Audit:

1. Login to the SharePoint Central Administration Console.
2. Go to the Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions"- this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. This account should be running as the Local system account

   Server Farm Standard Requirement
   a. This account should be a separate domain user account

   Server Farm using SQL Authentication
   a. This account should be a separate domain user account

   Server Farm using Doman user Authentication
   a. This account should be a separate domain user account

Remediation:

Single Server Set-Up
a. This account by default runs as the Local system account.

Server Farm standard requirement
a. Use a separate domain user account

Server Farm using SQL Authentication
a. Use a separate domain user account

Server Farm using Domain User Authentication

a. Use a separate domain user account.

All database accounts must be created as SQL Server login accounts in Microsoft SQL Server 2000 Enterprise Manager or SQL Server 2005 Management Studio. These accounts must be established before the creation of any content databases, including the configuration database and the `SharePoint_AdminContent` database. Create one SQL Server login for both the configuration database and the `SharePoint_AdminContent` database.

Additional Reference(s):
1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.7 Verify a Least Privileged Dedicated Setup User Domain Account (Level 1, Not Scorable)

Description:
Create a dedicated Setup User domain account and install SharePoint Server 2007 in server farm installations. The Setup User domain account is a required security account for SharePoint Server 2007. The account must be a member of the Administrators group on each Web front-end server and application server computer in the farm. On SQL servers, it must be a member of the SQL Server Service group with SQL Security administrator and database creator rights.

Rationale:
Ensure that the Setup User domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to the SharePoint Central Administration Console.
2. Go to the Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this which displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   <u>Single Server Set-Up</u>
   a. This account should be a member of the Administrators group on the local computer.

   <u>Server Farm Standard Requirement</u>
   a. This account should be a separate unprivileged Domain User account (NOT Domain Admin).
   b. This account should be a member of Local Administrators group on each server running the set-up.

c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Server Farm using SQL Authentication

a. This account should be a separate unprivileged Domain User account (NOT Domain Admin).
b. This account should be a member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Server Farm using Doman user Authentication

a. This account should be a separate unprivileged Domain User account (NOT Domain Admin).
b. This account should be a member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Remediation:

Single Server Set-Up

a. Member of the Administrators group on the local computer.

Server Farm standard Requirement

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Server Farm using SQL Authentication

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.
d. This account should NOT be a member of `securityadmin` and `dbcreator` fixed SQL Server role.

Server Farm using Domain user Authentication

a. Use a separate unprivileged Domain User account (NOT Domain Admin).
b. Member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Note: This account is used to configure databases. After each database has been created, change the database owner (`dbo` or `db_owner`) to the Setup User account.

Additional Reference(s)

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.8 Verify a Least privileged Dedicated Server Farm Domain Account (Level I, Not Scorable)

Description:

Create a least privileged dedicated Server Farm domain account in server farm installations. The Server Farm domain account, also referred to as a database access account, is the application pool identity for the SharePoint Central Administration Web site and the process account for the Windows SharePoint Services Timer service.

Rationale:

Ensure that the Server Farm domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to the SharePoint Central Administration Console.
2. Go to the Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions"- this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up

   a. No manual checking of the configuration is necessary.

   Server Farm Standard Requirement

   a. This account should be a separate domain user account.
   b. This account should be a member of Local Administrators group on each server running the set-up.
   c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

   Server Farm using SQL Authentication

   a. This account should be a separate domain user account.
   b. This account should be a member of Local Administrators group on each server running the set-up.
   c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

   Server Farm using Domain user Authentication

   a. This account should be a separate domain user account.

b. This account should be a member of Local Administrators group on each server running the set-up.
c. This account should NOT be a member of the Administrators group on the computer running SQL Server.

Remediation:

Single Server Set-Up

a. No manual configuration is necessary.

Server Farm standard requirement

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the server farm, including the computer running SQL Server.
c. This account does not require permissions to SQL Server before creating the configuration database.

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the server farm, including the computer running SQL Server.
c. NOT a SQL Server login on the computer running SQL Server.
d. This account does not require permissions to SQL Server before creating the configuration database.

Server Farm using Domain User Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the server farm, including the computer running SQL Server.
c. This account does not require permissions to SQL Server before creating the configuration database.

Note: After the Shared Services Provider (SSP) database and the SSP search database are created, add this account to the `Users` group and `db_owner` fixed database role.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.9 Verify a Least Privileged Dedicated Default Content Access account (Level 1, Not Scorable)

Description

Create a least privileged dedicated Default Content Access domain account in server farm installations. The Default Content Access domain account is used by the Windows SharePoint Services Search application server role to crawl content across sites.

Rationale
Ensure that the Default Content Access domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to → SharePoint Central Administration Console.
2. Go to → Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. No manual checking of the configuration is necessary.

   Server Farm Standard Requirement
   a. This account should be a separate domain user account.
   b. Check if the Office SharePoint Server Search service account used for Setup and running the configuration wizard has been changed to a domain user account.
   c. Remove the default content access account if it has been granted to the directory service.

   Server Farm using SQL Authentication
   a. This account should be a separate domain user account.
   b. This account should be a member of Local Administrators group on each server running the set-up.
   c. This account should NOT be a SQL Server login on the SQL Server Host.

   Server Farm using Doman user Authentication
   a. This account should be a separate domain user account.
   b. Check if the Office SharePoint Server Search service account used for Setup and running the configuration wizard has been changed to a domain user account.
   c. Remove the default content access account if it has been granted to the directory service.

Remediation:

Single Server Set-Up
a. No manual configuration is necessary.

Server Farm standard requirement

a. Use a separate domain user account.
b. By default, in a server farm environment, the Office SharePoint Server Search service account is used until a different account is specified. After completing Setup and running the configuration wizard, change this account to a domain user account.
c. Do not grant the default content access account access to the directory service.

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.
c. NOT a SQL Server login on the SQL Server Host.

Server Farm using Domain User Authentication

a. Use a separate domain user account.
b. By default, in a server farm environment, the Office SharePoint Server Search service account is used until a different account is specified. After completing Setup and running the configuration wizard, change this account to a domain user account.
c. Do not give the default content access account access to the directory service.

Note:

- For added security, use a different default content access account for each SSP.
- After the configuration database and the Central Administration content databases are created, add this account to the Users group and `WSS_Content_Application_Pools` database role for these databases

Additional Reference(s)

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.10 Verify a Dedicated Least Privileged Profile Import Default Access Account (Level I, Not Scorable)

Description:
Create a least privileged dedicated Profile Import Default Access domain account in server farm installations. The Profile Import Default Access domain account is used to connect to a directory service, such as the Active Directory service, a Lightweight Directory Access Protocol (LDAP) directory, a Business Data Catalog application, or other directory source and to import profile data from a directory service.

Rationale:
Ensure that the Profile Import Default Access domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to → SharePoint Central Administration Console.
2. Go to → Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments.

   Single Server Set-Up
   a. A manual checking of the configuration is not necessary.
   b. Check if the account uses the default Network Service.

   Server Farm Standard Requirement
   a. This account should be a separate domain user account.
   b. This account should NOT be a member of Administrators group on any computer in the server farm.

   Server Farm using SQL Authentication
   a. This account should be a separate domain user account.
   b. This account should NOT be a member of the Administrators group on any server in the farm, including the computer running SQL Server.
   c. This account should NOT be a SQL Server login.

   Server Farm using Doman user Authentication
   a. This account should be a separate domain user account.
   b. This account should have read access to the directory service and the Manage User Profiles personalization services permission

Remediation:

Single Server Set-Up

a. No manual configuration is necessary.
b. The account uses the default Network Service.

Server Farm standard requirement

a. Use a separate domain user account.
b. This account can be the same account as the default content access account, or use a separate account.
c. Read access to the directory service.
d. Manage User Profiles personalization services permission.
e. This account should not be a member of the Administrators group on any computer in the server farm.

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.
c. NOT a SQL Server login.

Server Farm using Domain User Authentication

a. Use a separate domain user account.
b. This account can be the same account as the default content access account or use a separate account.
c. Use an account that has read access to the directory service and the Manage User Profiles personalization services permission

Note: The Domain User account should not be a member of the Administrators group on any computer in the server farm.

Additional Reference(s)

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.11 Verify a Dedicated Least Privileged Windows SharePoint Services Search Service Account (Level I, Not Scorable)

Description:
In server farm installations, create a dedicated Windows SharePoint Services Search service domain account. The account is used as the service account for the Windows SharePoint Services Help Search service. It must be a domain user account and must not be a member of the Farm Administrators group.

Rationale:
Follow the principle of least privilege to ensure that the Windows SharePoint Services Search service domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to → SharePoint Central Administration Console.

2. Go to → Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. This account should run as the Local System account

   Server Farm Standard Requirement
   a. This account should be a separate domain user account.

   Server Farm using SQL Authentication
   a. This account should be a separate domain user account.
   b. This account should NOT be a member of the Administrators group on the computer running SQL Server.
   c. This account should NOT be a SQL Server login.

   Server Farm using Doman user Authentication
   a. This account should be a separate domain user account.

Remediation:

Single Server Set-Up

a. By default, this account runs as the Local System account.

Server Farm standard requirement

a. Use a separate domain user account.

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.
c. NOT a SQL Server login.

Server Farm using Domain User Authentication

a. Use a separate domain user account.
b. After the SSP database and the SSP search database are created, add this account to the Users group and `db_owner` role for each of these databases.

Note*:* when running the `Psconfig` command-line tool to start the Windows SharePoint Services Search service, membership is automatically configured in the following:

- `Users` group and `db_owner` role for the `WSS_Search` database.
- `Users` group in the configuration database.
- `Users` group in the Central Administration content database.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.12 Verify a Dedicated Least Privileged Windows SharePoint Services Search Content Access Account (Level I, Not Scorable)

Description:

In server farm installations, create a dedicated Windows SharePoint Services Search content access domain account. This account is used by the Windows SharePoint Services Search application server role to crawl content across sites. The account must be a domain user account and must not be a member of the Farm Administrators group.

Rationale:

Follow the principle of least privilege to ensure that the Windows SharePoint Services Search content access domain account is provided with only the minimum privileges needed to accomplish intended tasks. This practice follows the principle of least privilege by reducing the opportunity for a malicious user or process to affect the SharePoint environment. A malicious user will only have access to the compromised account's data.

Audit:

1. Login to → SharePoint Central Administration Console.
2. Go to → Operations tab.
3. Under Security Configuration section click on "Update farm administrator's group."
4. In the left pane select "Site Permissions" - this displays the Central Administration Permissions.
5. Note the user accounts with the permission.
6. Check and edit the permissions of the user account accordingly to the following environments:

   Single Server Set-Up
   a. This account should NOT be a member of the Farm Administrators group.

   Server Farm Standard Requirement
   a. This account should be a separate domain user account.

   Server Farm using SQL Authentication
   a. This account should NOT be a member of the Administrators group on any server in the farm, including the computer running SQL Server.
   b. This account should NOT be a SQL Server login.

Server Farm using Doman user Authentication

a. This account should be a separate domain user account.

Remediation:

Single Server Set-Up

a. Must not be a member of the Farm Administrators group.
b. Add to the Web application Full Read policy for the farm.

Server Farm standard requirement

a. Use a separate domain user account.

Server Farm using SQL Authentication

a. Use a separate domain user account.
b. NOT a member of the Administrators group on any server in the farm, including the computer running SQL Server.
c. NOT a SQL Server login.

Server Farm using Domain User Authentication

a. Use a separate domain user account.

Note: When running the `Psconfig` command-line tool to start the Windows SharePoint Services Search service, membership is automatically configured in the following:

- Users group and the `db_owner` role in the WSS— Search database.
- Users group in the configuration database.
- Users group in the Central Administration content database.

Additional Reference(s):

1. http://go.microsoft.com/fwlink/?LinkId=92931&clcid=0x409

1.1.13 Verify a Dedicated Single Sign-On (SSO) Accounts (Level I, Not Scorable)

Description:

Create the required Single Sign-On (SSO) accounts in order to set up, run, and administer the SSO system if the Microsoft SSO service is enabled in the SharePoint deployment.

Rationale:

These SSO accounts are responsible for managing various actions of the Single Sign-On service in SharePoint server 2007. They provide separation of roles and isolation of permissions; this helps track changes made to the SSO service.

Audit:

1. Ensure that the SSO account being created is authorized with the relevant permissions in the environment.
2. Do not use generic groups such as Authenticated Users, Power Users, and Users. Instead, create a new group exclusive to the SSO accounts only.

Remediation:

1. Plan the security environment
   The security guidance that is recommended for an organization depends on which environment best matches the intended use of Office SharePoint Server 2007.

2. Plan server farm security
3. Plan how to secure individual servers within a server farm. The patterns & practices security guides are used as a foundation for securing Office SharePoint Server 2007 environments.
4. Plan secure configurations for features
5. Plan how to configure Office SharePoint Server 2007 features in a secure manner.
6. Plan environment-specific security
7. Plan security targeted to the specific environment.
8. Plan security roles
9. A new feature in Microsoft Office SharePoint Server 2007 is a three-tier administrative model that centralizes configuration and management tasks, enables administrative roles to be differentiated, and administration to be delegated and assigned to the appropriate people in an organization.
10. Plan for single sign-on
11. When planning to connect to data sources outside of a server farm, single sign-on can be used to automatically authenticate users, rather than prompting for credentials.
12. Plan for accounts
13. It describes the accounts that must be planned for and describes the deployment scenarios that affect account requirements

Additional Reference(s):

1. http://technet2.microsoft.com/Office/en-us/library/3df68222-235b-45de-82fa-b89166c5c6bd1033.mspx?mfr=true

1.2 Installation and Configuration

This chapter provides recommendations for securely installing and configuring SharePoint Server 2007. Following recommendations in this section ensures that installations of the server are securely configured before intended use. If these recommendations are implemented the attack surface of the SharePoint Server 2007 is greatly reduced and offers users and documents increased protection against malicious activity.

1.2.1 Secure Windows 2003 Host Operating System (Level I, Not Scorable)

Description:
Apply the security guidance of the CIS Microsoft Windows Server 2003 Benchmark. Microsoft Windows Server 2003 is a core component of SharePoint Server 2007. The document provides recommendations for securely installing, configuring, and running the Server.

Rationale:

Ensuring Windows Server 2003 is installed and configured securely reduces the risk of the system being compromised.

Audit:
Follow the audit procedures articulated in the CIS Microsoft Windows 2003 Benchmark.

Remediation:
Refer to the security recommendations represented in the CIS Microsoft Windows 2003 benchmark. It establishes the latest best practices for securing the product and can be found at http://benchmarks.cisecurity.org/.

1.2.2 Secure IIS 6.0 Components (Level I, Not Scorable)

Description:
Microsoft Internet Information Service (IIS) is a core component of SharePoint Server 2007. Apply the security guidance from the CIS Microsoft IIS 5/6 Benchmark.

Rationale:
Ensuring IIS is installed and configured securely reduces the risk of the system being compromised.

Audit:
Follow the audit procedures articulated in the CIS Microsoft IIS 5/6 Benchmark.

Remediation:
Refer to the security recommendations represented in the CIS Microsoft IIS 5/6 benchmark. It establishes the latest best practices for securing the product and can be found at http://benchmarks.cisecurity.org/.

1.2.3 Secure Microsoft SQL 2005 Components (Level I, Scorable)

Description:
The Center for Internet Security offers guidance on securing SQL Server installations. Microsoft SQL Server is a core component of SharePoint Server 2007 and needs to be periodically configured and updated according to accepted standards.

Rationale:
Ensuring SQL Server is installed and configured securely reduces the risk of the system being compromised.

Audit:
Follow the audit procedures articulated in the CIS Microsoft SQL Server 2005 Benchmark.

Remediation:

Refer to the security recommendations represented in the CIS Microsoft SQL Server 2005. It establishes the latest best practices for securing the product and can be found at http://benchmarks.cisecurity.org/

1.2.4 SharePoint Server Hotfixes and Service Packs (Level I, Scorable)

Description:
Apply all SharePoint Server hotfixes and service packs.

Rationale:
Applying hotfixes and service packs protects the system against potential or known vulnerabilities. If the latest hotfixes and service packs are not applied then a malicious user could potentially compromise the system or might prevent certain functionality from being available.

Audit:
1. Go to: http://www.update.microsoft.com.
2. After the system is scanned for updates it should reflect no updates to be installed.

Remediation:
1. Go to: http://www.update.microsoft.com.
2. After the system is scanned and if install any Critical and/or Recommended updates.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/office/sharepointserver/bb735839.aspx

1.2.5 Central Administration Site Location (Level I, Not Scorable)

Description:
For environments that requires Internet-facing capability or in a two-server or more deployment, ensure that the Central Administration site is not hosted on a front-end Web server.

Rationale:
External malicious users could gain access to a front-end Web server, therefore the Central Administration web site should not be hosted on this server. If a malicious user gains access to the Central Administration site data could be compromised.

Audit:
1. On the Front end server check the following
2. Start → Search → Enter 'psconfig.exe' as the search string.
3. This file is the interface for Central Administration and should not be present.

Remediation:
On the Front end server check the following:
1. Start → Search → Enter 'psconfig.exe' as the search string.
2. If 'psconfig.exe' exists it means the interface for Central Administration is present on the same machine.
3. Depending on the feasibility either the Front End Server or the Central Administration web site should be moved to another machine.

In the case where an Internet-facing capability is required, two or more servers will be needed so that the Central Administration site will not be on the front-end Web server.

1.2.6 Central Administration Site Access (Level I, Not Scorable)

Description:
The Central Administration Site allows administrators to configure settings for SharePoint Server 2007. This site allows for farm as well as per-site configuration. Because this site is widely impactful to the server, it is prudent to block external access to the Central Administration site.

Rationale:
Blocking external access to the Central Administration site will help protect the Central Administration site against malicious external users. If the Central Administration site is not blocked from external users then sensitive data could be at risk.

Audit:
Try accessing the Central Administration Site using the URL (i.e. http://192.168.1.100:1084/_layouts/user.aspx).

The above page should not be accessible from a remote system.

Remediation:
Blocking external access to the Central Administration site can be achieved by placing a firewall between front-end Web servers and the server that hosts the Central Administration site. Configure the firewall with the following policies:

1. Disallow all HTTP access to the server hosting the Central Administration site.
2. Allow secure web access from the front-end Web server on the non-published port that the Central Administration site is listening on.

1.2.7 Enable Secure Sockets Layer (SSL) on the Central Administration site (Level I, Scorable)

Description:
Secure Sockets Layer (SSL) provides protection when communicating over the internet. Traffic is encrypted for portions of information transportation. Enable SSL on the Central Administration site.

Rationale:
The SharePoint Central Administration site allows an administrator to manage settings for the Web server and virtual servers. SSL protects this critical data by encrypting the traffic that is transmitted over the network.

Audit:
1. Start Internet Information Services (IIS) Manager.
2. Select the 'SharePoint Central Administration v3' and go to its properties.
3. On the Directory Security tab, in the Secure Communication section, click the 'Edit" button.
4. In the pop up window the *'Require secure channel (SSL)'* option should be checked.

Remediation:

Enable SSL for a virtual server by using Internet Information Services (IIS) Manager. A certificate must be acquired before enabling SSL. For more information about SSL certificates, see the topics About Certificates and Setting Up SSL on Your Server in IIS 6.0 Help.

Enable SSL in IIS:

1. Click Start, point to All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. Click the plus sign (+) next to the server name that contains the virtual server to change.
3. Click the plus sign (+) next to Web sites.
4. Right-click the virtual server and then click Properties.
5. On the Directory Security tab, under Secure Communications, click Edit.
6. In the Secure Communications dialog box, select the `Require secure channel` (SSL) check box, and then click OK.
7. Click OK again to close the Properties dialog box.

Additional Reference(s):

1. http://www.microsoft.com/resources/documentation/wss/2/all/adminguide/en-us/stse10.mspx?mfr=true

1.2.8 Limit Intranet IP Address in External DNS (Level I, Not Scorable)

Description:
Do not publish intranet IP addresses of SharePoint servers in the organization's external Domain Name System (DNS). Many SharePoint deployments will have Internet-facing servers publishing the same data with different security controls in place.

Rationale:
It is important to publish only the external IP addresses in DNS and not the intranet addresses. Publishing intranet addresses in an external Domain Name System would make the intranet addresses available to potential attackers.

Audit:
Execute the following from the command prompt:

```
nslookup all <name of the domain>.
```

Ensure that no internal IP is disclosed in the DNS record.

Remediation:

1. Edit the DNS Entries to remove internal IP addresses if any.

1.3 Central Administration

This chapter provides recommendations for the Central Administration site. The recommendations focus on the following areas: Security Operations, Application Management, SharePoint Web Application Management, SharePoint Site Management, User Profiles and My Sites, Office SharePoint Server Shared Services, and Shared Services Administration Search. In order to manage SharePoint through the Central Administration site, a user must login to the site as either a member of the server's local Administrators group or as a user configured as a SharePoint Administrator.

1.3.1 Change Single Sign-On (SSO) encryption key every 90 (Level I, Scorable)

Description:
Create a new Single Sign-On (SSO) encryption key every 90 days if the Microsoft SSO service is enabled in the SharePoint deployment. The encryption key encrypts and decrypts security credentials.

Rationale:
Create a new encryption key every 90 days limits, the amount of time that a compromised key can be used.

Audit:
The encryption key must be backed up each time a new key is created. It is not necessary to back up the encryption key at any other time (except when moving the encryption-key server role from one server to another). Back up the encryption key from the encryption-key server locally; the key cannot be backed up remotely.
Use encryption key backup and restore to move the encryption-key server role from one server to another. Other tasks must also be completed to move the encryption-key server role.

Remediation:
The first server that Microsoft Single Sign-On service (`SSOSrv`) is enabled on becomes the encryption-key server.

1. Login to the Encryption Key Server as the SSO Administrator.
2. Login to the Central Administration site as the SSO Administrator.
3. Select Operations → Security Configuration.
4. Select Manage settings for single sign-on.
5. Select Manage encryption key.
6. Select Create Encryption Key.
7. Check the box "Re-encrypt all credentials by using the new encryption key".
8. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc262932.aspx

1.3.2 Change SSO Encryption Key if Compromised (Level I, Not Scorable)

Description:

The SSO encryption key is used to encrypt and decrypt credentials that are stored in the SSO database. When suspicious that account credentials or the encryption key have been compromised, and the Microsoft Single Sign-On (SSO) service is enabled in the SharePoint deployment, create a new SSO encryption key and reencrypt user credentials in the SSO database with the new encryption key.

Rationale:
If account credentials and the encryption key are compromised by a malicious user, data on the system will not be secure. Changing the encryption key and reencrypting user credentials can protect the data from being compromised.

Audit:

1. If it is suspected that the SSO Key is compromised a new key should be generated and the following steps need to be followed before creating a new key.
2. The encryption key must be backed up each time a new key is created. It is not necessary to back up the encryption key at any other time (except when moving the encryption-key server role from one server to another). Back up the encryption key from the encryption-key server locally; the key cannot be backed up remotely.
3. Use encryption key backup and restore to move the encryption-key server role from one server to another. Other tasks must also be completed to move the encryption-key server role.

Remediation:
Since the reencryption process is a long running job, reencrypt credentials only at non-peak periods.

1. Login to the encryption-key server as the SSO Administrator.
2. Login to Central Administration as the SSO Administrator.
3. Navigate to Operations → Security Configuration.
4. Select Manage settings for single sign-on.
5. Select Manage encryption key.
6. Select Create Encryption Key.
7. Check the box "Re-encrypt all credentials by using the new encryption key".
8. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc261879.aspx

1.3.3 Host the SSO encryption key server on an Application Server (Level I, Not Scorable)

Description:
In a farm configuration, select an application server to host the SSO encryption key server if the Microsoft SSO service is enabled in the SharePoint deployment.

Rationale:

An application server computer is not directly accessed by end-users, and it is typically protected by additional layers of security, therefore making it the best choice to host the SSO encryption key server.

Audit:

1. Check if the SSO encryption key server exists on the Application Server through the following steps.
2. Login to the Application Server as the SSO administrator.
3. Go to Start → Run. Type `compmgmt.msc` and hit the Enter key.
4. Click on Services on the left panel.
5. Check if the "Microsoft Single Sign-on Service" is running on the server.

Remediation:

1. Configure SSO for Office SharePoint Server 2007
2. On Central Administration, on the top navigation bar, click Operations.
3. On the Operations page, in the Security Configuration section, click Manage settings for single sign-on.
4. On the Manage Settings for Single Sign-On page, in the Server Settings section, click Manage server settings.
5. On the Manage Settings for Single Sign-On page, in the Account name box in the Single Sign-On Administrator Account section, type the single sign-on administrator account name by using the form domain/group or domain/username.

Additional Reference(s)
1. http://technet.microsoft.com/en-us/library/cc261879.aspx

1.3.4 Manage the Single Sign-On (SSO) Encryption Key Server Locally Only (Level I, Not Scorable)

Description:
If the Microsoft SSO service is enabled in the SharePoint deployment, always login to the Single Sign-On (SSO) encryption key server locally when configuring or managing SSO.

Rationale:
Logging onto the encryption key server locally helps protect against network attacks. Since the data on the encryption key server is highly sensitive, it is critical to access this server only locally and not remotely.

Audit:
1. Ensure that the machine has access to the administrators locally only and NOT through remote connections. Set Windows Firewall to "On" with no exceptions for the following program/services:
2. File and Printer Sharing
3. Remote Assistance
4. Remote Desktop

Remediation:

The first server that Microsoft Single Sign-On service (SSOSrv) is enabled on becomes the encryption key server. The following steps describe how to access the SSO configuration items in Central Administration.

1. Login to the SSO encryption-key server as the SSO Administrator.
2. Login to Central Administration as the SSO Administrator.
3. Navigate to Operations → Security Configuration.
4. Select Manage settings for Single Sign-on.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc261879.aspx

1.3.5 Enable Secure Sockets Layer (SSL) (Level I, Scorable)

Description:
SSL protects the confidentiality of data while in transit between SharePoint servers and users. It is recommended that SSL be enabled.

Rationale:
Enabling SSL will ensure the confidentiality of sensitive information, such as usernames and passwords.

Audit:

1. Click Start, point to All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. Click the plus sign (+) next to the server name that contains the virtual server to change.
3. Click the plus sign (+) next to Web sites.
4. Right-click the virtual server and then click Properties.
5. On the Directory Security tab, ensure that "View Certificate" button is enabled.
6. Click on the "View Certificate" button to view and verify the certificate details.

Remediation:

1. Click Start, point to All Programs, point to Administrative Tools, and then click Internet Information Services (IIS) Manager.
2. Click the plus sign (+) next to the server name that contains the virtual server to change.
3. Click the plus sign (+) next to Web sites.
4. Right-click the virtual server and then click Properties.
5. On the Directory Security tab, under Secure communications, click Edit.
6. In the Secure Communications dialog box, select the `Require secure channel` (SSL) check box, and then click OK.
7. Click OK again to close the Properties dialog box.

Additional Reference(s):

1. http://www.sharepointblogs.com/tmt/archive/2008/01/30/configuring-ssl-in-sharepoint-2007-development-environment.aspx

1.3.6 Block potentially dangerous uploads (Level I, Scorable)

Description:
SharePoint can be configured to disallows uploads that end in specific file extensions. This feature of SharePoint prevents specified file types from being saved or retrieved from any site on the server. If a user attempts to save or retrieve a blocked file type, he or she will see an error and will not be able to save or retrieve the file.

Rationale:
The capability of blocking a file type mitigates the threat of users uploading undesirable files, such as malicious scripts and executables.

Audit:
1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Blocked file types.
4. Ensure at least each file type listed in the Remediation section is blocked.

Remediation:
1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Blocked file types.
4. Select a Web Application (or accept the default).
5. Block at least the following file types are blocked:

```
.ade, .adp, .app, .bas, .bat, .chm, .class, .cmd, .com, .cpl, .crt, .dll,
.exe, .fxp, .hlp, .hta, .ins, .isp, .jse, .lnk, .mda, .mdb, .mde, .mdt,
.mdw, .mdz, .msc, .msi, .msp, .mst, .ops, .pcd, .pif, .prf, .prg, .reg,
.scf, .scr, .sct, .shb, .shs, .url, .vb, .vbe, .vbs, .wsc, .wsf, .wsh,
```

6. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288335.aspx

1.3.7 Auditing Information Management Policy (Level I, Scorable)

Description:
The auditing information management policy is configured by default to be available in new site and list policies. Ensure that the auditing information management policy is configured to be available.

Rationale:
The auditing information management policy feature provides services for auditing user actions on documents and list in the Audit Log. Information in the Audit Log can assist in troubleshooting issues and determining accountability.

Audit:

1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Information management policy configuration.
4. Select Auditing.
5. Make sure the option “Available for use in new site and list policies” is checked.

Remediation:

1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Information management policy configuration.
4. Select Auditing.
5. Select the Status option "Available for use in new site and list policies".
6. Select Save.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc824908.aspx

1.3.8 Pluggable Authentication Provider (Level I, Not Scorable)

Description:

An authentication provider is a component that verifies user credentials. Configuring the authentication provider for a Microsoft Office SharePoint Server (MOSS) 2007 environment is an important security decision when setting up Internet-style SharePoint authentication. If external users require authenticated access to a SharePoint deployment, configure a pluggable authentication provider, which is a component that verifies user credentials.

Rationale:

Internal users can be verified through Windows authentication, while the pluggable authentication provider authenticates external users.

Audit:

1. Ensure that the Pluggable Custom Authentication configuration is not stored in clear text in the configuration files.
2. Ensure the account used for the authentication has the appropriate permissions in the SharePoint environment.

Remediation:

The following information from Microsoft provides an overview the MOSS membership providers. Visit Microsoft documentation for further guidance.

> “MOSS is built upon ASP.NET 2.0, which enables the use of pluggable authentication providers. This lets you use configurable directories for storing user information as long as there's an ASP.NET 2.0 membership provider (and optional role provider) that corresponds to the member data store. Pluggable provider credentials can be hashed, encrypted, or stored in plain-text depending on the node values stored in the `machine.config` file that correspond to the membership provider. Several membership providers are available for use with MOSS, some of which include an

LDAP V3 membership provider (which ships with MOSS), plus a SQL Server membership provider and Active Directory® membership provider available with ASP.NET 2.0.

The membership and role providers that can be implemented are not limited to the shipped providers. Using the ASP.NET 2.0 membership architecture, it is feasible to create custom providers that use membership stores like Microsoft Access or Oracle databases, XML files, or even flat text files. A custom authentication provider inherits from the ASP.NET `MembershipProvider` interface, which in turn inherits from the `ProviderBase` class.

There are some implications of using ASP.NET 2.0 authentication (as opposed to Windows authentication) with MOSS that should be taken into consideration. The most significant for many users is reduced Microsoft Office client interoperation resulting from the fact that the Web service communication between MOSS and Office clients was originally designed for use with Windows identities.

If you have a mandated PKI infrastructure based on security mechanisms such as smartcards where public keys or certificates are carried by clients, this typically requires that a Windows identity be resolved for proper client certificate acceptance and authorization, depending on implementation. This may, in turn, require creating an additional MOSS zone or other authentication configurations."

Additional Reference(s):

1. http://blogs.msdn.com/sharepoint/archive/2006/08/16/configuring-multiple-authentication-providers-for-sharepoint-2007.aspx

1.3.9 Configure antivirus settings (Level I, Scorable)

Description:
Configure antivirus settings to ensure that documents will be scanned for viruses upon download from and upload to the SharePoint Server.

Rationale:
Antivirus settings are not configured by default, leaving files downloaded from or uploaded to the SharePoint Server open to potential viruses. Checking for and removing malware will protect files and the SharePoint Server from becoming infected with malicious files.

Audit:

1. Open the Antivirus management Console.
2. Go to → Settings.
3. Check if antivirus scanning is enabled for both Incoming and Outgoing files from the machine.
4. The above steps are generic and not specific to any Antivirus application. An Antivirus application might have different terminology for the above context.

Remediation:
Follow these steps to configure antivirus settings:

1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Antivirus.
    a. Check the following boxes:
        i. Scan documents on upload
        ii. Scan documents on download.
    b. Attempt to clean infected documents.
4. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc261879.aspx

1.3.10 Information Rights Management (Level 2, Scorable)

Description:
Ensure that an Information Rights Management (IRM) solution has been installed and configured if documents need access control outside of the SharePoint environment. Once a document has been downloaded from a SharePoint site, its content generally is no longer protected unless some form of information rights management has been embedded in the document.

Rationale:
If a document contains highly sensitive information, provide embedded protection so that the information can be controlled regardless of where the document may be distributed. If such documents are protected by another means, IRM may not be needed. IRM allows content creators to control and protect their documents when disseminated outside of SharePoint in electronic form. IRM creates a set of access controls that live within the content and control access even when the document is outside of the SharePoint library.

Audit:
1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Information Rights Management.
4. Check if the "Use this RMS Server" is checked and an appropriate server is specified.

Remediation:
To configure Information Rights Management:

1. Login to Central Administration.
2. Navigate to Operations → Security Configuration.
3. Select Information Rights Management.
4. Select appropriate option.
5. Select OK.

Additional Reference(s):
1. Several vendors provide solutions. Microsoft provides the Windows Rights Management Services (RMS); see the following link:

http://technet2.microsoft.com/Office/en-us/library/073bfc71-7b01-4b77-bdc3-ac018889d54b1033.mspx?mfr=true

1.3.11 Prevents Users from Creating Connections Between Web Parts (Level I, Scorable)

Description:
Web Parts provide a means of connecting to data sources and integrating information from different data sources. Web Parts are custom pieces of code written by partners, IT, or individual developers. Enable the "Prevents users from creating connections between Web Parts, and helps to improve security and performance" option.

Rationale:
Web Parts can be unsafe or malicious. Following this recommendation can reduce the attack surface that a malicious web part can access. Specifically, Web Part connections allow Web Parts to discover and communicate to one another, up to and including access to sensitive information within each Web Part. Web Parts can be connected to libraries, lists, and to each other to reveal and manipulate data. Allowing users to create connections between Web Parts will increase the chance of a malicious code execution if the connecting Web Part being is from an unknown party. In the event that enterprise policy allows such connections, administrators should carefully consider which Web Parts to make available to.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Security for Web Part pages.
4. Check for each Web Application in the Web Application section check steps 5 and 6.
5. Check if the correct Web Application in the Web Application section.
6. Check if the "Prevents users from creating connections between Web Parts, and helps to improve security and performance" option in the Web Part Connections section.

Remediation:
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Security for Web Part pages.
4. For each Web Application in the Web Application section repeat steps 5-7.
5. Select the correct Web Application in the Web Application section.
6. Select the "Prevents users from creating connections between Web Parts, and helps to improve security and performance" option in the Web Part Connections section.
7. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc262665.aspx

1.3.12 Prevent users from accessing the Online Web Part Gallery (Level I, Scorable)

Description:
Enable the "Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance" option for each web application. Web Part galleries are groupings of Web Parts. There are four Web Part galleries: Closed Web Parts, Site Name Gallery, Server Gallery, and Online Gallery. The Online Gallery is a collection of Microsoft MSNBC Web Parts that are located on the Internet.

Rationale:
Due to the server attempting to connect to the MSNBC online gallery, allowing users to access the Online Web Part Gallery causes a significant performance hit to the server. This could result in a denial of service. The Online Gallery could contain web parts from unknown third parties, which could increase the risk of a malicious code execution attack. Preventing users from accessing the Online Web Part Gallery decreases the system's attack surface.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Security for Web Part pages.
4. Check for each Web Application in the Web Application section check steps 5 and 6.
5. Check if the correct Web Application in the Web Application section.
6. Check if the "Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance" option in the Online Web Part Gallery section.

Remediation
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Security for Web Part pages.
4. For each Web Application in the Web Application section repeat steps 5-7.
5. Select the next Web Application in the Web Application section.
6. Select the "Prevents users from accessing the Online Web Part Gallery, and helps to improve security and performance" option in the Online Web Part Gallery section.
7. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc262665.aspx

1.3.13 Disable Self-Service Site Creation (Level 2, Scorable)

Description:
The Self-Service Site Management page can allow users to create and manage their own top-level Web sites. Users can create top-level Web sites under a specific path (by default, the /sites path). When self-service site creation is enabled, an announcement is added to the top-level site at the root path of the Web application, and users who have permissions

to view that announcement can link to the new site. It is recommended that Self-Service Site Creation be disabled.

Rationale:
Allowing users to create sites as needed may increase the risk of inappropriate data handling and the SharePoint instance's attack surface.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Self-Service site management.
4. For each Web Application in the Web Application section repeat steps 5 and 6.
5. Navigate to Enable Self-Service Site Creation section.
6. Check if the option 'On' is selected.

Remediation:
To set the "Enable Self-Service Site Creation" option:
1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Self-Service site management.
4. For each Web Application in the Web Application section repeat steps 5-7.
5. Navigate to Enable Self-Service Site Creation section.
6. Select value [Off]
7. (Optional) Select `Require secondary contact`.
8. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc287817.aspx

1.3.14 Set List, Site and Personal Permissions as Appropriate (Level I, Not Scorable)

Description:
Ensure each web application is configured to provide only the required List, Site, and Personal permissions necessary for that web application. There are three sets of rights with individual permissions that are automatically applied for every new Web application that is created: List, Site, and Personal. List permissions include the standard user rights for viewing, adding, or deleting list items. For example, manage lists, edit items, delete items, approve items, and add items. Site permissions handle rights available on sites throughout the entire site collection. For example, the ability for a user to apply or change themes and borders or create groups and sub sites to a site. Finally, Personal permissions allow users to add or modify personalized Web Parts to sites.

Rationale:
Provide only the permissions necessary to use and manage the web application guards against erroneous use or modification of data.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select User Permissions for Web Application.
4. Under User Permissions for each Web Application ensure that the minimum user rights have been implemented

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select User Permissions for Web Application.
4. For each Web Application in the Web Application section repeat steps 5-7.
5. Select the next Web Application in the Web Application section.
6. Review all List, Site, and Personal permission lists and ensure the minimum user rights have been implemented.

Additional Reference(s):

1. http://office.microsoft.com/en-us/sharepointtechnology/HA011612141033.aspx

1.3.15 Set Access Rights per Zone (Level I, Not Scorable)

Description:

Policies are a new feature in SharePoint 2007. Ensure that users are granted the correct level of rights when accessing Web applications from a particular zone. The Policy for Web Applications tool enables administrators to create centralized policies that impact top-level site collections as well as sites configured in the Web application.

Rationale:

Administrators can create policies that determine the level of rights users are granted when connecting to a Web application from a specific zone. Examples of zones are Internet, Extranet, and Intranet. For example, if a user wanted to access a site on the Internet and download files, and there is a zone policy is in place which allows Read access only, that user is prohibited from downloading files. If policies are used, only the users who should have access to specific zones are granted access that provides the appropriate level of rights. Failure to verify this could result in data being exposed to unauthorized users.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Policy for Web Applications.
4. For each Web Application in the Web Application section repeat steps 5 and 6.
5. Select the Web Application of interest.
6. Ensure the user permissions are appropriate to their access.

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → Application Security.
3. Select Policy for Web Applications.
4. For each Web Application in the Web Application section repeat steps 5 and 6.

5. Select the Web Application of interest.
6. Verify user permissions.

Additional Reference(s):
1. http://www.microsoft.com/technet/technetmag/issues/2007/01/Security/default.aspx

1.3.16 Disable Anonymous Access (Level I, Scorable)

Description:
Disable anonymous access when creating or extending a SharePoint web application.

Rationale:
Anonymous access allows users to access a SharePoint Web site without authentication. However, the availability of anonymous access increases the susceptibility of the SharePoint deployment to malicious attacks. The default is for anonymous access to be disabled. In some cases, of course, a specific need to provide anonymous access may exist, such as an Internet facing deployment.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select `Create or extend Web application`.
4. Select `Create a new Web application or Extend an existing Web application`.
5. If extending an existing Web application, select the appropriate Web application.
6. Navigate to Security Configuration → Allow Anonymous.
7. Ensure Allow Anonymous value is set to [`No`].

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select `Create or extend Web application`.
4. Select `Create a new Web application or Extend an existing Web application`.
    a. If extending an existing Web application, select the appropriate Web application.
5. Navigate to Security Configuration → Allow Anonymous.
6. Select [`No`].
7. Enter other options with values appropriate to the deployment.
8. Select OK.

Additional Reference(s):
1. http://office.microsoft.com/en-us/sharepointtechnology/HA101130181033.aspx

1.3.17 Enable SSL for Web Applications (Level 1, Scorable)

Description:

SSL provides an added layer of security by encrypting and authenticating data that is transferred over a network connection. SSL is disabled by default for web applications.

Rationale:
If SSL is not in use, the data is not protected by encryption in transit and is potentially exposed a third party and results in integrity and confidentiality compromise.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select `Create or extend Web application`.
4. Select `Create a new Web application or Extend an existing Web application`.
   4.1. If extending an existing Web application, select the appropriate Web application.
5. Navigate to Security Configuration → Use Secure Sockets Layer (SSL).
6. Ensure use Secure Sockets Layers (SSL) value is set to [`Yes`].

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Create or extend Web application.
4. Select Create a new Web application if creating a new application, or Extend an existing Web application if extending an existing application.
5. If extending an existing Web application, select the appropriate Web application.
6. Navigate to Security Configuration → Use Secure Sockets Layer (SSL).
7. Select the option [`Yes`].
8. Enter other options with values appropriate to the deployment.
9. Select OK.

Additional Reference(s):
1. http://office.microsoft.com/en-us/sharepointportaladmin/HA011648191033.aspx

1.3.18 Use the "Delete Web Application" Capability (Level I, Not Scorable)

Description:
To completely delete the information associated with a SharePoint Web application use the "Delete Web Application" capability. The "Delete Web Application" capability can remove a Web application including its content databases. The "Remove SharePoint from IIS Web site" capability can be used to remove a site but does not provide the option to remove its content databases.

Rationale:
Using the "Delete Web Application" capability to remove the content databases protects against data leaks from the residual content databases that would be left by the "Remove SharePoint from IIS Web site" capability.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Delete Web application.
4. Select the Web Application to be deleted.
5. Ensure that the following are clicked under 'Deletion Options'
    a. Delete content databases.
    b. Delete IIS Web sites.

Remediation:
Consider backing up the web site and content databases before taking this action.

Caution: Deleting the content database and all IIS Web sites will also disable a non-SharePoint application that was sharing IIS Web site resources.

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Delete Web application.
4. Select the Web Application to be deleted.
5. Navigate to Deletion Options → Delete content databases.
6. Select [`Yes`].
7. Navigate to Delete IIS Web sites.
8. Select [`Yes`].
9. Select Delete.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288211.aspx

1.3.19 Use quota Templates (Level I, Not Scorable)

Description:
Ensure that an appropriate default quota template has been set for all site collections. Quota templates are used to specify the site storage size limit. By default, no quota template is selected for the default site collection of a new web application.

Rationale:
Uncontrolled growth of a site collection may degrade the performance of the deployment and even disrupt functionality. The selected template should be specified based on the types of sites being deployed and the capacity of the available hardware.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web application.
5. In the Default Quota Template section ensure a quota template is selected.
6. Ensure "Limit site storage to a maximum of:" under Storage Limit Values section is checked and an appropriate value is specified.

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web application.
5. Select Default Quota Template.
6. If an appropriate quota template exists, select it from the dropdown under "Select quota template" and go to step 11, otherwise continue with step 7 to create a new quota template.
7. Navigate to Default Quota Template.
8. Select `Quota Templates`.
9. Select `Create a new quota template`.
10. Enter a new name in the `New template name` textbox.
11. Navigate to the Storage Limit Values section:
    a. Check the checkbox to enable "Limit site storage to a maximum of:" and enter a value.
    b. Check the checkbox to enable "Send warning E-mail when site storage reaches:" and enter a value.
12. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288057.aspx

1.3.20 Set Security Validation to On (Level I, Scorable)

Description:
Verify that the "Security validation is" property is set to [On]. Without security validation being enabled, once a user authenticates, he or she will be able to access a site indefinitely in a given session.

Rationale:
Enabling validation reduces the chance that a page will be accessed by an unauthorized user while an authenticated user is absent. This setting forces the user to reauthenticate after a specified inactivity period is exceeded.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select a Web Application.
5. Navigate to Web Page Security Validation.
6. Ensure that the "Security validation is" property is set to [`On`].
7. Ensure that the "Security validation expires:" property is set to [`After`].

Remediation:
To verify that the "Security validation is" property is set to [`On`]:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select a Web Application.
5. Navigate to Web Page Security Validation.
6. Verify that the "Security validation is" property is set to [`On`].
7. Verify that the "Security validation expires:" property is set to [`After`].
8. Accept the default timeout period of 30 minutes or shorten it if appropriate.
9. If changes have been made, select OK, otherwise select Cancel.
10. Repeat steps 3 through 9 for each Web Application.

1.3.21 Configure the Policy for Profile Services (Level I, Not Scorable)

Description:
Configure the policy for profile services according to organizational policies. User profiles can display a broad range of information about the user, some of which may be sensitive.

Rationale:
Sensitive information should be displayed only to users that have a business need to see it. Policy for profile services determines which attributes are shown in user profiles and specifies which users can see each attribute.

Audit:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Site.
6. Select Profile services policies.
7. In the Manage Policy section, ensure the policy items are appropriately set.
8. Check steps 3-7 for each Shared Services Provider.

Remediation:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Site.
6. Select Profile services policies.
7. In the Manage Policy section, choose policy items for which the default values are not appropriate.
8. Select Edit policy and enter the new value. Otherwise, use the default values.
9. Select OK.
10. Repeat steps 3 through 9 for each Shared Services Provider.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc263080.aspx

1.3.22 Configure Default Reader Site Group for My Sites (Level I, Not Scorable)

Description:
When configuring My Site settings, include in the Default Reader Site Group only the accounts that require read access to future My Sites. The Default Reader Site Group specifies the accounts that will be added as Readers in created My Sites.

Rationale:
Changes to the Default Reader Site Group will affect only My Sites created after the change. Additionally, the default member of the Default Reader Site Group is the `NT AUTHORITY\authenticated users` group. If the user(s) of an included account does not have a need to know, the information at the My Sites could be compromised.

Audit:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Sites.
6. Select My Site settings.
7. Navigate to `Default Reader Site Group` section.
8. `NT AUTHORITY\Authenticated Users` group account should not exist if not required.
9. Ensure user and/or group accounts are set appropriately

Remediation:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Sites.
6. Select My Site settings.
7. Navigate to Default Reader Site Group section.
8. Remove the `NT AUTHORITY\Authenticated Users` group account if appropriate.
9. Add or remove user or group accounts, as appropriate.
10. Select OK.
11. Repeat steps 3 through 10 for each Shared Services Provider.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288314.aspx

1.3.23 Limit Shared Service Rights (Level I, Not Scorable)

Description:

Grant Shared Service Rights only to users that have a business need to manage shared services and grant to these users only the permissions for which they have a business need. Users that have Shared Service Rights can manage shared services.

Rationale:
Users not having a specific business need to manage shared services, such as "Manage User Profiles" and "Manage Permissions", may negatively affect the performance or the deployment and even stop it from functioning correctly. Following this recommendation implements the principle of least privilege, which generally reduces exposure to risk.

Audit:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Sites.
6. Select Personalization Services Permissions.
7. Ensure users and groups have the right privileges appropriate to their access.

Remediation:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to User Profiles and My Sites.
6. Select Personalization Services Permissions.
7. Remove unnecessary users and groups by checking the checkboxes next to them and selecting Remove Selected Users.
8. Repeat steps 9 through 12 for each remaining user and group.
9. Check the checkbox of the user or group.
10. Select Modify Permissions of Selected Users.
11. Ensure that the selected user or group has only the minimally required set of permissions, making changes as needed.
12. Select OK.
13. Repeat steps 4 through 12 for each Shared Services Provider.

    If additional users or groups are needed, ensure that each has only the minimally required set of permissions when adding them (using "`Add Users/Groups`").

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc262918.aspx

1.3.24 Limit URL's in Search Results (Level I, Not Scorable)

Description:

Enter into the "URLs to remove" textbox any URLs that should not appear in search results. The specified URLs will be removed from search results immediately when the “Remove Now” button is clicked. Additionally, crawl rules will be created to exclude the specified URLs from future crawls.

Rationale:
The "URLs to remove" text field is used to specify the URLs that should be removed from search results. The existence of some SharePoint resources, such as sites, documents, or lists, should be known only to users who have a business need to know. Displaying the URLs of such resources in search results reveals their existence, which may also suggest what information is held in that resource.

Audit:
To check whether the search results are displaying any unintended authorized information for a particular search query follow the steps below:

1. Go to SharePoint Search
2. Enter the search string to get the results and ‘Search’

If the results include the URL’s which map to unintended disclosed documents, sites, lists use the ‘Enter the URLs to remove’ option to remove the URL’s intended not to be public.

Remediation:
1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to Search.
6. Select Search settings.
7. Select Search result removal.
8. Enter the URLs to remove in the URLs to remove text field.
9. Select Remove Now.

This recommendation should be implemented each time the path to a new sub site containing sensitive information needs to be excluded from the search results.

Additional Reference(s):
1. http://msdn.microsoft.com/en-us/library/bb896018.aspx

1.3.25 Specify a Quota Template when Creating a Top-level Web site (Level I, Not Scorable)

Description:
Ensure that a quota template has been set on top-level web sites for each web application. Quota templates manage site and server resources.

Rationale:

A quota template identifies the amount of storage allocated for a given site. If no storage limit is set, a site could use so many resources that other sites will not be able to function properly.

Audit:

1. Login to Central Administration.
2. Navigate to Component Configuration → Manage quota and locks → Manage Quota Templates
3. In the Template name area, select Edit an existing template
4. In the Template box, select the quota template to change.
5. In the Storage Limit Values section, ensure that the values for Limit site storage to a maximum of: ___ MB check box has been set.

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Site Management.
3. Select Create site collection.
4. Fill in all the required fields to create a new top-level Web site.
5. Either define a new quota template by selecting `Manage Quota Templates`, or select a predefined template, and ensure that storage limit values are set appropriately.
6. Select OK.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc288057.aspx

1.3.26 Disable "Automatically delete the site collection if use is not confirmed" property (Level 2, Scorable)

Description:

Verify that the "Automatically delete the site collection if use is not confirmed" property is not enabled for each web application. Automatic deletion is an administrative feature that will remove unused sites without administrative intervention and a backup mechanism. Automatic deletion permanently removes all content and information from the site collection and any sites beneath it.

Rationale:

If the site collection administrator or secondary site collection administrator fails to confirm a site is still in use when receiving an email notification asking if the site is still in use, the site is automatically deleted. This could result in a denial of service to the users of that site. Data could be lost if a backup was not made prior to removing the site collection.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Site Management.
3. Select Site use confirmation and deletion.
4. Repeat the following steps for each web application:
5. Select the Web Application.

6. Ensure that the "Automatically delete the site collection if use is not confirmed" checkbox is not checked.

Remediation:
To verify that a Web application has not been setup for automatic deletion, do the following:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Site Management.
3. Select Site use confirmation and deletion.
4. Repeat the following steps for each web application:
5. Select the Web Application.
6. Uncheck the "Automatically delete the site collection if use is not confirmed" checkbox

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288481.aspx

1.3.27 Define a Secondary Site Collection Administrator (Level 2, Scorable)

Description:
Define a secondary site collection administrator when creating a new site collection. If a site reaches its maximum size, users will be denied access until an administrator fixes the problem. Having a secondary administrator reduces the risk of having a denial of service on a site.

Rationale:
If the site reaches its maximum size, the secondary administrator can fix the problem if the primary administrator is not available. In some situations, having a secondary site administrator could be inappropriate for reasons of control or confidentiality.

Audit:
1. Login to Central Administration.
2. Go to Home page, click Site Action menu → Site Settings.
3. On the Site settings page →Users and Permissions section → Site Collection administrators.
4. On the Site Collection administrator page, in the text box with the users (separated by semicolons) ensure there is a second administrator.

Remediation:
1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Site Management.
3. Select Create site collection.
4. Fill in all the required fields to create a new top-level Web site.
5. Define a Secondary Site Collection Administrator.
6. Select OK.

Additional Reference(s):
1. http://office.microsoft.com/en-us/sharepointserver/HA101577811033.aspx

1.3.28 Set SMTP Mail Server (Level I, Scorable)

Description:
Identify the SMTP mail server in the outgoing e-mail settings. E-mail messages are sent to site administrators when a site approaches its maximum size.

Rationale:
If the outgoing e-mail server has not been identified in the e-mail settings, no e-mail will be sent to site administrators to fix the problem. If a site reaches its maximum size, users will be denied access to the site.

Audit:

1. Login to Central Administration.
2. Navigate to Operations → Topology and Services.
3. Select Outgoing e-mail settings.
4. Ensure that the mail settings have been set for
    a. Outbound SMTP server field
    b. From address
    c. Reply-To address
    d. Character set.

Remediation:
SMTP must be installed on the server (in this case Windows Server 2003) in order for SharePoint to send the emails.

1. Login to Central Administration.
2. Navigate to Operations → Topology and Services.
3. Select Outgoing e-mail settings.
4. Enter the SMTP server in the Outbound SMTP server field.
5. In the `From` address box, enter the address as it should appear to e-mail recipients.
6. In the `Reply-to address` box, enter the e-mail address that recipients will reply to.
7. In the `Character set` menu, select the appropriate character set.
8. Select OK.

1.3.29 Specify Search "exclude" Crawl Rules. (Level I, Not Scorable)

Description
Verify that URLs that should not appear in search results are specified in "exclude" crawl rules. The Manage Crawl Rules window specifies URLs to include or exclude from the crawl. It shows a list of URLs that have been specified to be included or excluded in the crawl.

Rationale:
The existence of some SharePoint resources, such as sites, documents, or lists, should be known only to users who have a business need to know. Displaying the URLs of such

resources in search results reveals their existence, which may also suggest what information is held in that resource.

Audit:
To check whether the search results are displaying any unintended authorized information for a particular search query follow the steps below:

1. Go to SharePoint Search.
2. Enter the search string to get the results and 'Search.'

If the results include the URL's which map to unintended disclosed documents, sites, lists change the Crawl rules appropriately.

Remediation:
1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select shared service to manage.
4. Login to the service.
5. Navigate to Search.
6. Select Search settings.
7. Select Crawl Rules.
8. Verify that the list of exclude rules includes all the URLs that should not appear in search results.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc262934.aspx

1.3.30 Do not allow External Users to Participate in Workflows (Level 2, Scorable)

Description:
Set the "Allow external users to participate in workflow by sending them a copy of the document?" option to [`No`]. When selected, a user who has no access to the SharePoint site can receive a copy of a document as an email attachment.

Rationale
Unauthorized users should not be allowed in an environment in which documents may contain sensitive information. This option enables a workflow configuration so that an external user can receive a copy of a document as an email attachment.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management → Workflow Management.
3. Select Workflow settings.
4. Select a Web Application.
5. Navigate to Workflow Task Notifications.
6. Ensure that the option "Allow external users to participate in workflow by sending them a copy of the document?" is set to [No].

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → Workflow Management.
3. Select Workflow settings.
4. Select a Web Application.
5. Navigate to Workflow Task Notifications.
6. Select the [No] option for "Allow external users to participate in workflow by sending them a copy of the document?"
7. Select other options as desired.
8. Select OK.
9. Repeat steps 3 through 8 for each Web Application.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc263399.aspx

1.3.31 Limit the Right to Create Personal Web Sites (Level I, Scorable)

Description:

Only grant the right to 'Create personal site' to users that have a business need. By default, all authenticated users can create a My Site. This recommendation grants this right only to users having a business need to have such a site.

Rationale:

Allowing all users to have personal sites increases the risk of inappropriate or extraneous content. The implementation of this recommendation has the potential to increase the security of the deployment and to improve performance.

Audit:

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select Shared Services Provider.
4. Select Personalization services permissions.
5. Check the box "`NT AUTHORITY\Authenticated Users`" group.
6. Select Modify permissions of selected users.
7. Ensure the check box for 'Create personal site' is unchecked.

Remediation:

Follow steps 1-8 to remove the 'Create personal site' permission from `NT AUTHORITY\Authenticated Users` group.

1. Login to Central Administration.
2. Navigate to `Shared Services Administration`.
3. Select Shared Services Provider.
4. Select Personalization services permissions.
5. Check the box `NT AUTHORITY\Authenticated Users` group.
6. Select Modify permissions of selected users.
7. Uncheck box 'Create personal site'.

8. Select Save.

Follow these steps to grant specific users the right 'Create personal site'.

1. Select Add Users/Groups.
2. Navigate to Choose Users.
3. Enter users and group names.
4. Navigate to Choose permissions.
5. Check Create personal site.
6. Select Save.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc263483.aspx

1.3.32 Anti-Virus Scanning For Downloaded Documents (Level I, Scorable)

Description:
Check documents for viruses upon download.

Rationale:
Configuring antivirus settings ensures that documents will be scanned for viruses upon download from and upload to the SharePoint server. Antivirus settings are not configured by default, therefore leaving the documents downloaded from or uploaded to SharePoint open to potential viruses.

Audit:

1. Login to Central Administration
2. Navigate to Operations > Security Configuration.
3. Select Antivirus.
4. Check the following box: Scan documents on download.
5. Select OK.

Remediation:

1. Login to Central Administration
2. Navigate to Operations > Security Configuration.
3. Select Antivirus.
4. Ensure that the “Scan documents on download” box is checked.

1.3.33 Cleaning Infected Documents (Level I, Scorable)

Description:
Ensure documents are scanned for viruses when uploading and downloading from the server.

Rationale:
Configuring antivirus settings ensures that documents will be scanned for viruses upon download from and upload to the SharePoint server. Antivirus settings are not configured by default, therefore leaving the documents downloaded from or uploaded to SharePoint open to potential viruses.

Audit:

1. Login to Central Administration.
2. Navigate to Operations > Security Configuration.
3. Select Antivirus.
4. Check the following box: Attempt to clean infected documents
5. Select OK.

Remediation:

1. Login to Central Administration.
2. Navigate to Operations > Security Configuration.
3. Select Antivirus.
4. Ensure the “Attempt to clean infected documents” box is checked.

1.4 Site Administration

This chapter provides recommendations that are implemented at the Site level. The SharePoint Server allows configuration of sites at a global or granular level. Secure guidance in this section is geared towards acceptable user permissions, group permissions, information management, and information management policies. Appropriately configuring these ensures user and data protection.

1.4.1 Do Not Crawl Sensitive Content (Level 2, Scorable)

Description:
A crawler connects to and reads information to create entries for a search engine index. SharePoint includes a crawler that extracts data from various content sources. Configure the server to exclude sensitive content from the SharePoint crawl.

Rationale:
Regardless of whether a user has permission to view a source, a user can view the results of crawled content of all sources matching queried search criteria. The listing of restricted content in search results can lead to information disclosure. Individual documents, lists, sites, etc., that are excluded from the crawl become unavailable for searching by users who are authorized to view the sources.

Audit:

1. Check at the site level:
2. Navigate to Site Actions → Site Settings → Modify All Site Settings → Site Administration.
3. Select Search Visibility.
4. Navigate to `Allow this web to appear in search results`.
5. Ensure that the option [`No`] is selected.
6. To check the Exclude content in a list or library from search results:
7. Select the list or the library that contains content that should not appear in search results.
8. Navigate to the Settings menu.
9. Select Document Library Settings for a library or List Settings for a list.
10. Navigate to General Settings.
11. Select Advanced Settings.
12. Navigate to Search.
13. Ensure that the option [`No`] is selected.

Remediation:

At the site level:

1. Navigate to Site Actions → Site Settings → Modify All Site Settings → Site Administration.
2. Select Search Visibility.
3. Navigate to `Allow this web to appear in search results`.

4. Select the option [No].
5. Select OK.

Exclude content in a list or library from search results:

1. Select the list or the library that contains content that should not appear in search results.
2. Navigate to the Settings menu.
3. Select Document Library Settings for a library or List Settings for a list.
4. Navigate to General Settings.
5. Select Advanced Settings.
6. Navigate to Search.
7. Select the option [No].
8. Select OK.

Additional Reference(s):
1. http://support.microsoft.com/kb/932619

1.4.2 Set the "Auto-accept requests?" property to [No] (Level I, Scorable)

Description:
Set the "Auto-accept requests?" property to `[No]` when creating new site groups. If auto-accept is enabled in Site Settings, users will automatically be added to the site group when they make a request to join the group. Users will have the permissions of the group to which they are added and this might include access to sub sites.

Rationale:
The “Auto-accept requests” property deprives the site owner, the control over who becomes a member of the group, thereby enabling frivolous use of the site. Groups that are specifically designed to allow public membership should have the ''Auto-accept requests?'' property set to `[Yes]`.

Audit:
While creating a New Group under a Site ensure that the option “Auto-accept requests” is set to [No].

Remediation:
At the site level:

1. Navigate to Site Actions → Site Settings → People and groups.
2. On the New dropdown list, select New Group.
3. On the New Group Page:
4. Enter Name and About Me Description.
    a. Enter Owner.
    b. Configure Group Settings options.
    c. Navigate to Membership Requests section.
    d. Set the "`Allow requests to join/leave this group?`" property to `[Yes]` or `[No]` as appropriate for the site.

e. Navigate to Auto-accept requests? section.
f. If the "`Allow requests to join/leave this group?`" property has been set to `[No]`, the "auto-accept requests?" property options are disabled and the property defaults to `[No]`; otherwise, select `[No]`.
g. In the Give Group Permission to this Site section, set the group permissions as appropriate.

5. Select Create.

Additional Reference(s)

1. http://office.microsoft.com/en-us/sharepointserver/HA101032221033.aspx

1.4.3 Allow only Group Owners to Edit Group Membership (Level I, Scorable)

Description:

Set the "Who can edit the membership of the group?" property to [`Group Owner`] when creating new site groups.

Rationale:

Adding and removing group members may have security implications for the sites in which that group has access. Inadvertent addition or deletion of members to or from groups may endanger the security of the site. Only the owner of the group should have this capability. Careless addition or removal of group members in a group can have negative security implications for the sites to which that group has access. If only the owner of the group has the capability to edit membership of the group, the risk of having undesired members in the group is significantly reduced.

Audit:

While creating a New Group under a Site ensure that the option "Who can edit membership of the group" is set to [`Group Owner`].

Remediation:

1. At the site level:
2. Navigate to Site Actions → Site Settings → People and Groups.
3. Select New.
4. Select New Group from drop down list.
5. On the New Group Page:
    a. Enter Name and About Me Description.
    b. Enter Owner.
    c. Configure Group Settings options.
    d. Navigate to `Who can edit membership of the group?` section.
    e. Select [`Group Owner`].
6. Select Create.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc288338.aspx

1.4.4 Restrict who can View Group Membership (Level 2, Scorable)

Description:
Set the "Who can view the membership of the group?" property to a value other than `Everyone`.

Rationale:
In some situations, knowing the membership of a group can reveal other sensitive information. This might be the case in a collaborative environment in which people from different functional organizations are members of the same group to accomplish a team objective. In such a case, knowing the membership of the group could reveal some part or their entire objective, which may be sensitive information.

Audit:
While creating a New Group under a Site, ensure that the option "View membership of the group" is no set to `Everyone`.

Remediation:

At the site level:

1. Navigate to Site Actions → Site Settings → People and Groups.
2. Select New.
3. Select New Group from drop down list.
4. On the New Group Page:
    a. Enter Name and About Me Description.
    b. Enter Owner.
    c. Configure Group Settings options.
    d. Navigate to `Who can view membership of the group?` section.
    e. Select `[Group Members]`.
5. Select Create.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288440.aspx

1.4.5 Create information management policies (Level I, Not Scorable)

Description:
Create information management policies. Information management policy usage reports can contribute to an understanding of how records are managed and whether users are complying with policy. This is especially relevant for organizations that must comply with legal or regulatory requirements. For example, a Human Resources policy, used in an organization to ensure that employee records are handled in accordance with legally recommended guidelines, could include the features such as auditing, retention period, and labels for physical copies.

Rationale:
Information management policy usage reports are enabled by the administrator for Central Administration, while specific information management policies are created by site

administrators. Naturally, if policies are not relevant to the organization's activities and records management, the information management policy usage reports may be superfluous.

Audit:
Ensure that information management policies are in place by the following steps:

1. Go to Site Actions → Site Settings → Modify All Site Settings → Site Collection Administration.
2. Select Site collection policies.
3. Ensure that the required policies are listed for a particular site collection.

Remediation:
At the top-level site:

1. Navigate to Site Actions → Site Settings → Modify All Site Settings → Site Collection Administration.
2. Select Site collection policies.
3. Select Create.
4. Enter Name, Administrative Description, and Policy Statement text.
5. Check one or more of the policy enabling checkboxes, such as Enable Labels, as appropriate for the policy being created, and complete the specific entries needed for the checked items.
6. Select OK.

Additional Reference(s):
1. http://office.microsoft.com/en-us/sharepointserver/HA101735291033.aspx

1.4.6 Ensure Best Bets Do Not Reveal Sensitive Information (Level I, Not Scorable)

Description:
Verify that existing Best Bets do not reveal sensitive information. Best Bets are associated with keywords and their synonyms. A Best Bet is a link to the information that is highly relevant to the keyword or one of its synonyms. When a keyword is used in a search by a user, the Best Bet location appears on the search results page. This directs users to items the enterprise administrator has identified as most appropriate.

Rationale:
However, in some situations the existence of the Best Bet (that is, the target information that the user will be directed to) should not be revealed to users who are not authorized to access that information. In such a situation, the Best Bet potentially compromises sensitive information. Since content may be added to document libraries or lists, an existing Best Bet might unintentionally reveal sensitive information.

Audit:

1. Navigate to the top-level site of the site collection.

2. Navigate to Site Actions → Site Settings → Modify All Site Settings.
3. Navigate to Site Collection Administration.
4. Select Search keywords.
5. Select a Keyword, under the Keyword column, and choose Edit in the dropdown.
6. Navigate to Best Bets on the Edit Keyword page.
7. Review and ensure that the listed Best Bets do not point to sensitive information.
8. Check steps 5-7 for each existing Best Bet.

Remediation:
Follow these steps to review Best Bets and to verify that they do not point to sensitive information:

1. Navigate to the top-level site of the site collection.
2. Navigate to Site Actions → Site Settings → Modify All Site Settings.
3. Navigate to Site Collection Administration.
4. Select Search keywords.
5. Select a Keyword, under the Keyword column, and choose Edit in the dropdown.
6. Navigate to Best Bets on the Edit Keyword page.
7. Review and verify that the listed Best Bets do not point to sensitive information. To see the URL and Description associated with a Best Bet, select Edit in the row of the Best Bet.
8. If a Best Bet points to sensitive information, select Remove in the row of the Best Bet.
9. Select OK if any Best Bets have been removed, otherwise Select Cancel.
10. Repeat steps 5-9 for each existing Best Bet.

Additional Reference(s)
1. http://support.microsoft.com/kb/923900

1.5 Backup and Recovery

This chapter provides recommendations for backing up and recovering SharePoint Server 2007 deployments. Guidance in this chapter refers to content recovery and disaster recovery as though they are separate capabilities. General opinion is often that disaster recovery is inclusive of content recovery. However, Microsoft published a paper [Reference 3] in which three levels of recovery are used: content recovery, site recovery, and disaster recovery. Content recovery generally refers to capabilities such as document versioning and the two-stage recycle bin. These capabilities are targeted to specific content and can be managed by individual users in addition to site administrators. The Microsoft paper characterizes content recovery as a frequent and small-scale activity. Site recovery refers to tools used to recover from accidental deletion or data corruption of a site. This kind of recovery is performed by site administrators. Disaster recovery methods generally refer to global backup and recovery, involving sites or farms, under the control of a farm administrator. This terminology serves the practical purpose of being suggestive of scope and is used in this chapter.

1.5.1 Backup the Single Sign-On (SSO) Encryption Key (Level I, Not Scorable)

Description:
Backup the Single Sign-On (SSO) encryption key each time a new key is created if the Microsoft SSO service is enabled in the SharePoint deployment.

Rationale:
The Single Sign-On encryption key is used to encrypt and decrypt user credentials. Users will experience a denial of service if the encryption key becomes corrupt and there is no backup of the key.

Audit:
Document the path where the Encryption Key is backed up in the Recovery Plan document. Use the same to check if the BackUp file exists is current. If not, proceed with the new back up file.

Remediation:
Note: The first server that Microsoft Single Sign-On service (SSOSrv) is enabled on becomes the encryption-key server.

1. Login to the Encryption Key Server as the SSO Administrator.
2. Login to Central Administration as the SSO Administrator.
3. Navigate to Operations → Security Configuration.
4. Select Manage settings for single sign-on.
5. Select Manage encryption key.
6. Navigate to Encryption Key Backup.
7. Under Drive, select the removable disk drive on which to store the encryption-key backup.
8. Select Back Up.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc512096.aspx

1.5.2 Configure document versioning (Level I, Not Scorable)

Description:
Document versioning is the native versioning functionality for document libraries in SharePoint Server 2007. Enabling document versioning provides a layer of defense against data corruption and erroneous changes made by users.

Rationale:
Document versioning creates history for a document each time a document is saved. Therefore, a document that becomes corrupt can be restored to a previous version. However, document versioning neither prevents deletion of documents nor protects the content of documents. For example, this recommendation will not protect against conditions of heavy use in which several users create edited versions of many documents. This can produce excessive document versioning which consumes resources.

Audit:
Check if the document versioning has been set by following the steps:

1. Navigate to Site Actions → Site Settings → Modify Pages Library Settings → General Settings.
2. Select Versioning settings.
3. Ensure the versioning options are appropriately set for the selected site.

Remediation:
SharePoint Server 2007 offers versioning options, which can be controlled separately for each document library. The Versioning Settings page is located under Document Library Settings. "Managing Document Versioning," page 318 (Reference 1) suggests that the best practice is to configure site templates to have predefined document libraries with versioning options preset according to organizational policy. Modifying a site and saving it as a new template is one method. Using SharePoint Designer 2007 is another method. Its features enable more flexible deployment of functionality within SharePoint. Master Pages make changing the look and feel of sites in SharePoint easy. The Document Center template, provided with SharePoint 2007, has versioning set to track both major and minor versions.

There are two ways to set the versioning options for a document library on a given site. Use whichever one happens to be most convenient. First, for a document library on a given site:

1. Navigate to Site Actions → Site Settings → Modify Pages Library Settings → General Settings.
2. Select Versioning settings.
3. Set the versioning options appropriately for the selected site.

Second, versioning settings can also be reached from the Document Library:

1. Select the Document Center tab on the home site.
2. In the left pane (Site Hierarchy), select Documents.
3. Navigate to Settings → Modify Pages Library Settings → General Settings.
4. Select Versioning settings.
5. Depending on business needs, select either Create major versions or Create major and minor (draft) versions.
6. Set the number of versions to retain. Keep as few versions as possible to minimize storage needs.
7. Select OK.

Additional Reference(s)

1. http://technet.microsoft.com/en-us/library/cc263011.aspx

1.5.3 Two-stage Recycle Bin (Level I, Scorable)

Description:

Verify that the two-stage feature of the recycle bin is not disabled. In the first-stage, also known as the "user-stage," Recycle Bin provides an undelete feature that allows end users with appropriate permissions to recover accidentally deleted files, documents, list items, lists, and document libraries from a site. The second-stage, also known as the "site-collection stage," Recycle Bin is located at the site collection administrator level.

Rationale:

The two-stage recycle bin is a convenient, easy to use method for restoring deleted files, and is enabled by default. When an item is deleted from the first-stage Recycle Bin, it can only be recovered by a site collection administrator from the second-stage Recycle Bin. If disabled, all content in the recycle bin is removed, freeing up the disk space, which may help when storage space is low.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select a Web Application.
5. Scroll down to the options for the recycle bin.
6. Ensure Recycle Bin Status option is `[On]`.
7. Ensure Second stage Recycle Bin option is not `[Off]`.
8. Repeat steps 4-7 for each web application.

Remediation:

To verify options for the two-stage recycle bin:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select a Web Application.
5. Scroll down to the options for the recycle bin.
6. Set Recycle Bin Status option to `[On]`.

7. Set Second stage Recycle Bin option to `[On]`.
8. Repeat steps 4-7 for each web application.

1.5.4 Back up SharePoint 2007 (Level I, Not Scorable)

Description:
Back up the SharePoint 2007 deployment.

Rationale:
Having a backup of the SharePoint deployment is critical for disaster recovery. Without an appropriate backup, the SharePoint deployment would have to be reconstituted practically from scratch and much or all of the former content could be lost.

Audit:
Ensure that the Share Point Back up is taken at regular intervals to successfully make a recovery.

Remediation:
Office SharePoint Server provides two built-in backup and recovery tools: Central Administration and the stsadm.exe command-line tool. Third-party tools are also available, but not covered in this recommendation.

Central Administration provides an easy way to back up the Office SharePoint Server system at various levels, the highest level is the farm and the lowest is a content database.

1. Login to Central Administration.
2. Navigate to Operations → Backup and Restore.
3. Select Perform a backup.
4. Select Farm.
5. Select Continue to Backup Options.
6. Specify the type of backup (full or differential) and the backup location.
7. Select OK.

The "stsadm.exe" command-line tool offers options to back up an entire farm, a site collection, or an item. This method of backup and recovery is processor intensive, may use large amounts of storage, and does not scale well. However, for a single server or for small farms it is a reasonable line of defense for disaster recovery.

1. Open a command window on the server.
2. Change directory to the location of stsadm.exe (e.g., `cd C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\BIN`).
3. To display all operations available in the tool type "stsadm.exe -help".
4. To get help on backup type "stsadm.exe -help backup".

Additional Reference(s):
1. Refer to documentation on stsadm.exe; for example, see Command-Line Operations in the Windows SharePoint Services Administrator's Guide at

http://www.microsoft.com/resources/documentation/wss/2/all/adminguide/en-us/stsk01.mspx?mfr=true

2. Also, see the example in Reference 1, Chapter 30, page 1086.

1.5.5 Backup IIS Metabases (Level I, Not Scorable)

Description:
Backup SharePoint-related Internet Information Services (IIS) Metabases regularly.

Rationale:
The Metabase contains the IIS configuration data, which supports Intranet/Internet-related SharePoint activity. Thus, regular backups are important to continuity of operations.

Audit:
Ensure that the IIS Metabase Backup is taken on a regular basis.

Remediation:
Although the Metabase is included in system-state backups done with the Windows Server Backup/Restore Wizard, the restoration action restores the entire system, including the system registry. This is unacceptable if only the Metabase needs to be restored.

To create a portable backup (password required):

1. In IIS Manager, right-click the local computer, click All Tasks, and then click Backup/Restore Configuration.
2. Click Create Backup.
3. In the Configuration backup name box, type a name for the backup file.
4. Select the Encrypt backup using password check box, type a password into the Password box, and then type the same password in the Confirm password box.
5. Click OK, and then click Close.
6. The IIS metabase is created in the `%systemroot%\system32\inetsrv\MetaBack` folder.

To create a non-portable backup (password not required)

1. In IIS Manager, right-click the local computer, click All Tasks, and click Backup/Restore Configuration.
2. Click Create Backup.
3. In the Configuration backup name box, type a name for the backup file.
4. Click OK, and then click Close.
5. The IIS metabase is created in the `%systemroot%\system32\inetsrv\MetaBack` folder.

Additional Reference(s):

1. http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/131b609d-ff3a-488f-a8dd-13044fa623a1.mspx?mfr=true

1.5.6 Backup the SSO Database (Level I, Not Scorable)

Description:

Back up the SSO database after the initial install and then again each time the credentials are re-encrypted if the Microsoft SSO service is enabled in the SharePoint deployment.

Rationale:
Creating backups will help prevent a denial of service if the SSO database becomes corrupt. If the database is not backed up after reencrypting credentials, restoring the database will result in bad credentials.

Audit:
Ensure that the backup of the SSO database is taken before the credentials are reencrypted due to enabling the Microsoft SSO Service.

Remediation:
1. Login to Central Administration.
2. Navigate to Operations → Backup and Restore.
3. Select Perform a backup.
4. Check the SSO box.
5. Select Continue to Backup Options.
6. Select Full or Differential for the Type of Backup.
7. Enter the Backup location.
8. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us /library/cc512096.aspx

1.5.7 Single Sign-On (SSO) Encryption Key Backup (Level I, Not Scorable)

Description:
Do not store the backup media for the Single Sign-On (SSO) encryption key in the same location as the backup media for the SSO database if the Microsoft SSO service is enabled in the SharePoint deployment.

Rationale:
If a user obtains a copy of both the SSO database and the encryption key, the credentials stored in the database could be compromised.

Audit:
Ensure that the backup media for the SSO encryption key and the backup for the SSO database are stored on different locations.

Remediation:
1. Backing Up the encryption key
2. On Central Administration, on the top navigation bar, click Operations.
3. On the Operations page, in the Security Configuration section, click Manage settings for single sign-on.
4. On the Manage Settings for Single Sign-On page, in the Server Settings section, click Manage encryption key

5. On the Manage Encryption Key page, in the Drive list in the Encryption Key Backup section, click the removable media drive on which to store the encryption-key backup.
6. Click Back Up.
7. Back Up the encryption key in a different location from the SSO database back up.

Additional Reference(s)

1. http://technet.microsoft.com/en-us/library/cc512096.aspx

1.5.8 Recycle Bin (Level I, Scorable)

Description:

Ensure that the recycle bin is `[On]` and set an appropriate value for the retention period based on the available disk space. The recycle bin helps to prevent the loss of erroneously deleted data. By default, the recycle bin is `[On]` and has "Delete items in the Recycle Bin:" set to `[After 30 days]`.

Rationale:

When the recycle bin is turned `[On]` in a Web application, each site in this application has its own separate recycle bin. To prevent uncontrolled growth of disk space consumed by recycle bins, a retention period must be specified at the Web application level.

Audit:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web Application.
5. Navigate to the Recycle Bin section.
6. Ensure 'Recycle Bin Status' is set to [On].
7. Ensure 'Delete items in the Recycle Bin' is set to [After] and an appropriate value for the retention period is entered.
8. Select OK.
9. Repeat steps 2-6 for each web application.

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management → SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web Application.
5. Navigate to the Recycle Bin section.
6. Under Recycle Bin Status select [On].
7. Under Delete items in the Recycle Bin select [After] and enter the appropriate value for the retention period.
8. Select OK.
9. Repeat steps 2-6 for each web application.

1.5.9 Back up critical sites (Level I, Not Scorable)

Description:
Backing up sites for which loss of content must be avoided is a good defense against loss of items that have been emptied from the second-stage recycle bin and loss of web pages that have been deleted from a site collection.

Rationale:
Having a backup of a site would recover the site quickly instead of performing full farm level restores.

Audit:
Ensure that the network team has a schedule planned to take back-up of critical sites at regular intervals. For example, windows scheduler can be used to perform any customized back-up job at regular intervals saving time while preparing for data loss.

Remediation:
Administrators can use Office SharePoint Designer 2007, Microsoft IT Site Delete Capture 1.0, a database snapshot, or the stsadm.exe tool to back up and recover Web sites.

Office SharePoint Designer 2007 is a Microsoft product that can be purchased. See the Designer home page at http://office.microsoft.com/en-us/sharepointdesigner/FX100487631033.aspx. Office SharePoint Designer 2007 provides the ability to back up and restore site collections, down to the individual file level. Backing up a Web site with this tool creates a content migration package (.cmp file).

Note: The backup file does not include objects in the Recycle Bin.

MSIT Site Delete Capture 1.0 is a free tool available at http://go.microsoft.com/fwlink/?LinkID=92682&clcid=0x409. When a site is deleted, Office SharePoint Server generates a Web Delete event. Microsoft IT (MSIT) created Microsoft IT Site Delete Capture feature 1.0 to detect and act on the Web Delete event. When a Web Delete event is detected, the feature archives the site to a file share before it is removed from the configuration and content databases.

Note: This tool is not part of Office SharePoint Server, and may not be updated. This tool is built on supported Microsoft technologies, but it is not supported by Microsoft.

A SQL Server snapshot is a read-only view of a database as the database existed at the time that the snapshot was created. For more information about using snapshots with Office SharePoint Server, see this article in the Microsoft Knowledge Base: "How to use SQL Server to take a snapshot of a Windows SharePoint Services 3.0 content database" (http://go.microsoft.com/fwlink/?LinkID=99636&clcid=0x409).

Note: The snapshot version of a Web site does not have full functionality; for example, files cannot be written or uploaded to the snapshot version.

The `stsadm.exe` tool is part of SharePoint 2007. The `stsadm.exe` tool can be used to backup and recover small farms using its backup and recover options. This method of backup and recover is processor intensive, may use large amounts of storage, and does not scale well. However, for small farms it is a reasonable line of defense for disaster recovery.

To use this tool:
1. Open a command window on the server.
2. Change directory to the location of `stsadm.exe` (e.g., `cd C:\Program Files\Common Files\Microsoft Shared\web server extensions\12\BIN`).
3. To display all operations available in the tool type "`stsadm.exe –help`."

To get help on backup run:

```
stsadm.exe -help backup
```

Additional Reference(s):
1. Refer to documentation on stsadm.exe; for example, see Command-Line Operations in the Windows SharePoint Services Administrator's Guide at http://www.microsoft.com/resources/documentation/wss/2/all/adminguide/en-us/stsk01.mspx?mfr=true
2. Also, see the example in Reference 1, Chapter 30, page 1086.

1.5.10 Recycle Bin Retention Period (Level I, Not Scorable)

Description:
Ensure an appropriate value for the recycle bin retention period is set based on available disk space.

Rationale:
The recycle bin helps to prevent the loss of erroneously deleted data. By default, the recycle bin is [On] and has "Delete items in the Recycle Bin:" set to [After 30 days]. When the recycle bin is turned [On] in a Web application, each site in this application has its own separate recycle bin. To prevent uncontrolled growth of disk space consumed by recycle bins, a retention period must be specified at the Web application level.

Audit:
1. Login to Central Administration.
2. Navigate to Application Management > SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web Application.
5. Navigate to the Recycle Bin section.
6. Under Recycle Bin Status select [On].
7. Under Delete items in the Recycle Bin select [After] and enter the appropriate value for the retention period.
8. Select OK.
9. Repeat steps 2-6 for each web application.

Remediation:

1. Login to Central Administration.
2. Navigate to Application Management > SharePoint Web Application Management.
3. Select Web application general settings.
4. Select Web Application.
5. Navigate to the Recycle Bin section.
6. Ensure Recycle Bin Status is set to [On].
7. Ensure Delete items in the Recycle Bin select [After] value is set for the retention appropriate period.

1.6 Logging and Reporting

The SharePoint Server logs and records a variety of events such as server operations and status. Such logging and reporting includes: diagnostic, execution, trace logs, application, and performance logs. This chapter contains recommendations on configuring the logging and reporting functionality of the SharePoint Server.

1.6.1 Diagnostic Logging (Level 1, Not Scorable)

Description
The diagnostic logging feature in Central Administration sets thresholds for logging and reporting events associated with user activities. Set the diagnostic logging thresholds appropriately for the particular SharePoint deployment.

Rationale
Logging extensive information assists in identifying issues or trends. However, logging all possible information can have a degrading effect on the performance of a SharePoint Server. Setting the appropriate logging threshold ensures appropriate information is captured while maintaining the performance integrity of the system.

Audit

1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic logging.
4. Ensure that an appropriate Event Throttling option is selected.

Remediation
To set the logging thresholds:

1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic logging.
4. Select appropriate Event Throttling options.
5. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc288649.aspx

1.6.2 Information Management Policy Usage Reports (Level I, Not Scorable)

Description:
Information management policy usage reports contribute to an understanding of how records management is managed and whether users are complying with policy. To facilitate the audit of acceptable usage, enable information management policy usage reports.

Rationale:
Information Management Policy Usage Reports are relevant for organizations that must comply with legal or regulatory requirements. For example, a Human Resources policy

used in an organization to ensure that employee records are handled within legally recommended guidelines could include the features such as auditing, retention period, and labels for physical copies. If policies are not relevant to the organization's activities and records management, the information management policy usage reports may be superfluous.

Audit:

1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Information management policy usage reports.
4. Select a Web Application.
5. Navigate to Schedule Recurring Reports.
6. Ensure that the check the box for "Enable recurring policy usage reports" is checked.
7. Ensure that the scheduling time for the reports is appropriately set for the intended SharePoint operations.
8. Ensure that an appropriate Report File Location is set.

Remediation:

1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Information management policy usage reports.
4. Select a Web Application.
5. Navigate to Schedule Recurring Reports.
6. Check the box for "Enable recurring policy usage reports".
7. Set the options here appropriately for the intended SharePoint operations.
8. Navigate to Report File Location.
9. Enter an appropriate URL in the Report file location: textbox.
10. Navigate to Report Template and specify the template to use for creating reports.
11. Select OK.
12. Repeat steps 2 through 11 for each Web Application.

Information management policies are defined by site administrators. To create an information management policy on a site:

1. Login to or open the top-level site.
2. Select Site Actions.
3. Select Site Settings.
4. Select Modify All Site Settings.
5. Navigate to Site Collection Administration.
6. Select Site collection policies.
7. Select Create.
8. Enter Name, Administrative Description, and Policy Statement text.
9. Check one or more of the policy enabling checkboxes, such as Enable Labels, as appropriate for the policy being created and complete the specific entries needed for the checked items.

10. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc263021.aspx

1.6.3 Disable Error Report Collection (Level 2, Scorable)

Description:
SharePoint can be configured to send Microsoft information regarding errors that SharePoint has encountered. The intent of this capability is assist Microsoft and its partners in identifying and resolving problems in SharePoint. It is recommended that this option be disabled.

Rationale:
An error report may contain sensitive information such as part of a document you were working on or data that you recently submitted to a website.

Audit:
1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic Logging.
4. Ensure that the 'Collect error reports' checkbox is checked to create error reports when the system encounters hardware of software problems.

Remediation:
1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic Logging.
4. Check the Collect error reports checkbox.
5. Select OK.

Additional Reference(s):
1. http://technet.microsoft.com/en-us/library/cc263021.aspx

1.6.4 Single Sign-On (SSO) Service Logging (Level I, Scorable)

Description:
If the Microsoft SSO service is enabled in the SharePoint deployment, enable logging for the Single Sign-On service. Logging SSO events facilitates accountability and assists in determining suspicious activity on a system.

Rationale:
Changes to databases cannot be audited if SSO events are not logged and periodically reviewed.

Audit:
1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic logging.

4. Navigate to Event Throttling.
5. Ensure SSO is selected in the Select a category dropdown list.
6. Ensure that an appropriate level in the Least critical event is selected to report to the event log dropdown list.
7. Ensure that an appropriate level in the Least critical event is selected to report to the trace log dropdown list.

Remediation:

1. Login to Central Administration.
2. Navigate to Operations → Logging and Reporting.
3. Select Diagnostic logging.
4. Navigate to Event Throttling.
5. Select SSO in the Select a category dropdown list.
6. Select an appropriate level in the Least critical event to report to the event log dropdown list.
7. Select an appropriate level in the Least critical event to report to the trace log dropdown list.
8. Select OK.

Additional Reference(s):

1. http://technet.microsoft.com/en-us/library/cc263280.aspx

1.7 SharePoint Extensions

This SharePoint Extensions chapter provides recommendations to secure the SharePoint Server when using third-party functionality. This reference provides minimal recommendations and is considered to be peripheral to the scope of this document. For additional information on this subject, review the references provided within recommendations.

1.7.1 Use Strong-names for Web.config [SafeControl] Entries (Level 1, Scorable)

Description:

The `Web.config` file gives the administrator control over which assemblies are permitted to run on a virtual server. Only assemblies identified by a `<SafeControl>` entry are allowed. Use fully qualified assembly names when adding a `[SafeControl]` entry to the `Web.config` file. An assembly's name is stored in metadata and has a significant impact on the assembly's scope and use by an application. A strong-named assembly has a fully qualified name that includes the assembly's name, culture, public key, and version number. This is frequently referred to as the display name, and for loaded assemblies can be obtained by using the `FullName` property. This information is used at runtime to locate the assembly and differentiate from other assemblies with the same name.

Rationale:

A partially qualified assembly name identifies only the name of the assembly. A fully qualified assembly name also identifies version number, culture, and developer identity. Using fully qualified assembly names in a `<SafeControl>` entry provides important information that can be used in security policies based on content-based evidence.

Audit:

1. To view the fully qualified names of assemblies in the global assembly cache using the .NET Framework Configuration tool
2. Go to Start → Control Panel → Administrative Tools → Microsoft .NET Framework Configuration.
3. Click Manage the Assembly Cache, and then click View List of Assemblies in the Assembly Cache.
4. Ensure that the usage of fully qualified assembly names in the `<SafeControl>` entry in the `web.config` file.

Remediation:

1. Open the `web.config` and ensure that the `Assembly` attribute of each `SafeControl` entry contains the assembly's name, version, culture, and non-null public key token.

Additional Reference(s):

1. http://msdn2.microsoft.com/en-us/library/k8xx4k69.aspx

1.7.2 Ensure processRequestInApplicationTrust is set to false (Level I, Scorable)

Description:

Set the `processRequestInApplicationTrust` attribute of the `[trust]` element to `[false]`. This attribute controls whether an application's `PermitOnly` stack walk modifiers will be in effect during execution. When set to `[true]`, the Page class uses the `PermitOnly` stack walk modifier on the ASP.NET permission set.

Rationale:
Granting more extensive permissions via a policy file is made useless. The default setting for SharePoint environments is `[false]` while the default setting for ASP.NET is `[true]`. Setting the attribute to `[false]` enables the use of custom security policy files.

Audit:
In the <`trust`> element of a `Web.config` file, ensure that the attribute is set:

```
processRequestInApplicationTrust="false"
```

Remediation:
In the `<trust>` element of a `Web.config` file, set the attribute to:

```
processRequestInApplicationTrust="false".
```

1.7.3 Permissions on ASP.NET Applications (Level I, Not Scorable)

Description:
Grant ASP.Net applications the minimum permissions necessary.

Rationale:
ASP.Net applications running on the SharePoint server run at a default permission level of `WSS_Minimal` which provides only the minimum permissions necessary to run effectively on the SharePoint system. However, administrators or application developers can install custom-developed ASP.Net applications and assign a custom trust level to those applications. If the trust level assigned to these applications is greater than necessary, malicious individuals could use these trusted applications to gain unauthorized access to (or perform undesirable actions on) the rest of the SharePoint system.

Audit:
Set permissions for ASP.NET applications to appropriate levels.

Remediation:
Review web applications and ensure appropriate permissions and trust levels.

2 Notes and Warnings

This chapter provides notes and warnings for administrators regarding SharePoint Server 2007.

2.1.1 Web Application Security Testing and Configuration

Before configuring security options on a Web application, plan and test the configuration. For example, test settings such as the user rights for Web application for general access before users are added to the operational site.

2.1.2 Usage Analysis Processing

Usage analysis processing produces log files, such as number of page hits for each page, number of unique users, browser and operating system information, and referring domains and Uniform Resource Locator (URL). This information assists in identifying issues that may cause a denial of service to users.

2.1.3 Web Application User Permissions

User permissions, rights, and policies for individual Web applications are defined in the Application Security section of the Central Administration tool. Ensure the correct Web application is selected in the management control before defining these permissions, or valid users may be prohibited from performing their required roles.

2.1.4 Web Application Permission Levels

Disabling and re-enabling permission levels for a Web application in the Central Administration GUI instantly modifies permissions in all site collections contained in the selected Web application. Be cautious when making changes to large Web applications because every site collection contained within it is also modified by the system. This modification could cause a large increase in CPU utilization, which may cause a denial of service. (Reference 6.)

2.1.5 Inheriting Permissions from Parent Sites

If Use Same Permissions as Parent Site is selected, one set of user permissions is shared by both the parent and a new site. Consequently, user permissions on the new site can only be changed by an administrator of the parent site. Any changes made to the permissions on a parent site will propagate throughout the site hierarchy to any sub sites inheriting permissions from a parent. This potentially may lead to a site attaining permissions that are not appropriate for one or more of an inheriting sub sites.

2.1.6 Third Party Web Parts

Third-party Web Parts that require a full permission set to execute successfully are often not well designed. Carefully consider the acquisition and integration of Web Parts.

3 Appendix A: References

Reference 1: Bill English with the Microsoft SharePoint Community Experts, 2007, Microsoft Office SharePoint Server 2007: Administrator's Companion, Library of Congress Control Number: 2006937020, Microsoft Press, Redmond, Washington 98052-6399.

Reference 2: Curry, B., 2007, Microsoft SharePoint Products and Technologies: Administrator's Pocket Consultant, ISBN:9780735623828, Microsoft Press, Redmond, Washington 98052-6399.

Reference 3: Lanceleaux, B. and Office SharePoint Server 2007 Content Publishing, October 2007, Date protection and recovery for Microsoft Office SharePoint Server 2007 in small to medium-sized deployments, available at Microsoft Technet, Microsoft Office System, Office SharePoint Server 2007 (http://technet2.microsoft.com/Office/en-us/library/32a18803-52d2-4967-ab9d-0e199c9bf0041033.mspx?mfr=true), Microsoft Corporation.

Reference 4: Microsoft TechNet, June 28, 2007, Administering backup and recovery for Office SharePoint Server 2007, http://technet2.microsoft.com/fwlink/?LinkId=102627andamp;clcid=0x409, Microsoft Corporation.

Reference 5: Microsoft TechNet, June 28, 2007, Prepare to back up Office SharePoint Server 2007, http://technet2.microsoft.com/Office/en-us/library/620dc024-8dfe-4c4c-8bb4-2ff0cfa84a311033.mspx, Microsoft Corporation.

Reference 6: Office IT and Servers User Assistance (o12ITdx@microsoft.com), June 2007, Microsoft Office SharePoint Server 2007 Office SharePoint Server Security, Microsoft Corporation.

4 Appendix A: Change History

Date	Version	Changes for this version
December 5th, 2011	1.0.0	Public Release