Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

Auditing a Windows 2000 Active Directory Infrastructure:
An Auditor's Perspective

Auditor: Sylvia Choa

May 2003
Version 1.3

Table of Contents

Table of Figures

INTRODUCTION

This paper evaluates the risks to a Windows 2000 Active Directory infrastructure, of a chosen company and network. Based on the evaluation, a checklist is created for hardening the security of the chosen system, meeting the industry best practices, and hence minimizing the company's risks. A series of tests are conducted on risks that are deemed most critical, by the Information Technology Security and Architecture Directory of the company.

The intended audiences for this document are auditors of information network and systems, security and system administrators, who are familiar with Windows 2000 Active Directory.

Assignment 1 – Research in Audit, Measurement, Practice and Control

The IS component being audited and its role in the organization.

I am auditing a Windows 2000 Active Directory (AD) and its environment, for ABC Entertainment Ltd ('*The Company*'). There are two distinct areas of security being addressed in *The Company*'s new Windows 2000 network infrastructure – external access to *The Company* and internal control over access to *The Company*'s resources. Like most Windows 2000 implementations *The Company* is using its Windows 2000 AD to manage most, if not all, of its internal security infrastructure.

The project of the Windows 2000 AD being audited is currently in its deployment phase, to users at the Head Office. It is envisaged that the implementation at the Head Office will be completed within the next few weeks. The primary objective of this audit is to certify the security design for and of the AD, to ensure it will comply with *The Company*'s security policies and procedures, and be in line with the industry's best practice. The ultimate goal is to ensure the AD domains will never become unavailable because of policy-related issues. The findings and recommendations from this audit will form the basis for addressing any deficiencies in the original AD security design, prior to the full implementation throughout the remaining offices.

In this particular case the AD structure and Organizational Units (OU) design are based on *The Company*'s business requirements and future enterprise administrative and management goals, namely: improved scalability, reliability and manageability. The AD directory service provides *The Company* the structure and functions for organizing, managing, and controlling their network resources, which are strategically and logically grouped by OU. It also enables their administrators to manage their Windows 2000 network from a central

location. Group policies are used to specify the security settings for desktops, users, servers and domain controllers. Delegation of administrative control over AD objects, such as user or computer accounts, is based on the individuals' administrative roles and responsibilities for the AD, as per The Company's support structure.

In order to provide a resilient, robust and secure solution, *The Company* has built redundancy into the core Windows 2000 network. There are two Root Domain Controllers (RDC) and two Active Directory Domain Controllers (ADC) in the Head Office Domain. The peer or redundant RDC and ADC are housed in a separate computer room in a separate premise, from the primary RDC and ADC.

The external access to *The Company* and other stand-alone and member servers are outside the scope of this audit. As shown in Figure 1, *The Company* is using Microsoft ISA servers to allow for tight integration of Internet and remote access security with the Windows 2000 AD. Firewalls are used to provide a security layer between *The Company* and the outside world. The following network diagram shows the main components of the Windows 2000 network infrastructure being audited.

Figure 1 – High Level Network Diagram
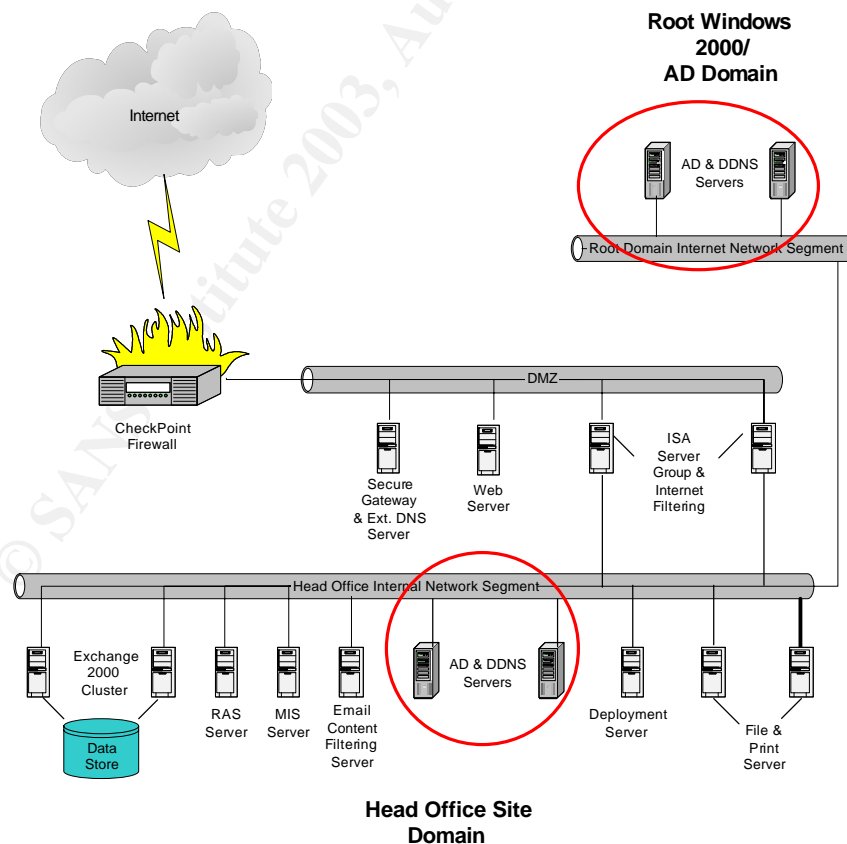
The scope of this audit is indicated by the circles in Figure 1, that is, the AD and its environment.

Evaluate the risk to the system

Based on the high level network diagram (Figure 1) and interviews with key architects who were responsible for the design and/or implementation of the AD, I concluded that security is one of the most important success criteria to *The Company* for its Windows 2000 Solutions Framework implementation, which includes a Windows 2000 AD infrastructure.

To demonstrate the importance of security to its future business strategies, *The Company* has replaced its old firewall with Nokia Firewall, and a DMZ was also implemented, as shown in Figure 1.

> "The Nokia Firewall/VPN appliance offers an unbeatable combination: market-leading Check Point firewall/VPN technology on a purpose-built, hardened Nokia platform with a security-specific operating system (IPSO)."[1]

These security measures are put in place to defend against attacks aimed at the internal network of *The Company*. Overall there is evidence of "defence in depth" in the entire security design.

Having strong perimeter protection against external hacking alone is inadequate in protecting an organisation's information technology (IT) infrastructure. To complete the security framework, organisations also need to put in place strong internal security controls and procedures against inside/internal hack. One must not underestimate the damage that can be caused by internal hack. A recent event, whereby an Australian security firm was forced to cease trading after an internal hack, has proved once again how damaging internal hack can be. As reported in ComputerWorld NZ, Wednesday, 12 March, 2003:

> "Aust security firm goes under after inside hack" – heading
>
> ""Stunned" is how the head of a New Zealand integrator describes the demise of Australian security software distributor Janteknology, which ceased trading after a damaging internal hack." [2]

The Company recognised that Windows 2000 AD security and the internal processes, policies and procedures governing user access to its network and the internet, are equally important. Therefore, within the scope of this audit, the main areas for investigation are namely, (a) AD security, and (b) internal processes/policies/procedures that are put in place to enhance security for the AD infrastructure. Anything else is outside the scope of this audit. Beware that this is not a full audit of Windows 2000 Server.

---

[1] http://www.nokia.com/nokia/0,5184,151,00.html

[2] http://computerworld.co.nz/webhome.nsf/printdoc/2907E0C36EA81521CC256CE5006B1117!opendocument

Active Directory (AD) Security

Risk 1.1	Inadequate protection for the Domain Controllers.
Probability	High
Impact	Failure of a domain controller, especially if fault tolerance does not exist, will stop domain authentication from working.
Priority	Critical
Control Objectives	Since Domain controllers contain sensitive data used for authentication, its availability must be maintained at all time.

Risk 1.2	Lack of clearly defined roles and responsibilities for the administration of the AD, and inappropriate delegation of control for the administration of the AD.
Probability	Medium
Impact	Poor management for the AD infrastructure, which could have high impact on the availability of the AD domain. Potentially, there will be a lack of accountability for changes occurred and ownership for problems resolution, resulting in poor service delivery to the users of the AD infrastructure.
Priority	Critical
Control Objectives	Integrity of the AD and its availability must be maintained. Administrative roles and responsibilities must be clearly defined. The ability of individuals to perform certain AD administrative functions must be appropriately controlled.

Risk 1.3	Access to MMC consoles not restricted, and not in line with the AD administrative roles and responsibilities.
Probability	Medium
Impact	If delegation of administration is lacking or incorrectly configured, an intruder with full control of the admin tools could exploit the admin privileges to gain further details about the internal network; for launching an attack.
Priority	Low
Control Objectives	The integrity and availability of the AD must be maintained. The risk of an intruder gaining full control of the admin tools must be minimized. Access to MMC snap-ins must be restricted based on the roles and responsibilities for the AD.

Risk 1.4	Default AD access permissions and NTFS ACLs are too permissive, granting **Everyone** group **Full Control** permissions on the root of each logical disk volume on the AD, and newly created file shares and registry keys.
Probability	High
Impact	Vulnerability of domain controller to disk-space attacks on each

	disk volume, including the AD database files volume. Inappropriate access permissions assigned to file shares and registry keys.
Priority	Low (if the Guest account has been disabled)
Control Objectives	Unauthorised access to file shares and registry keys must be minimized. NTFS file system must be used. Appropriate ACLs must be applied to the registry keys, file system and other data (and log) partitions; in order to maintain the stability and integrity of the AD infrastructure.

Risk 1.5	Domain Controllers not kept up-to-date with the latest Service Packs and security Hotfixes.
Probability	High
Impact	Exposure to known security threats, through unauthorised access to the system, with elevated privileges at the server level.
Priority	Critical
Control Objectives	Exposure to security threats must be minimized.

Risk 1.6	Inadequate account and password policies, permitting the use of weak passwords and accounts that never get locked out. Weak passwords are easily exploited by intruders, making possible a denial of service attack or unauthorized access to proprietary information.
Probability	High
Impact	Potential loss of system availability and integrity, and unauthorised access to confidential corporate data. Also potential loss of credibility.
Priority	Critical
Control Objectives	Must have strong password policy in place. Systems must be configured to force all passwords to meet the complexity requirements. Screen saver must have password enabled. To enhance security, different passwords should be used on each server in a workgroup or domain. The Administrator account password must contain at least one nonalphanumeric character in the first seven characters.

Risk 1.7	Domains and Domain Controllers not secured by appropriate GPO settings.
Probability	High
Impact	Incorrectly configured GPOs could open up security holes to the AD and the internal network. This could have adverse impact on the stability, integrity and availability of the AD.
Priority	Critical

Control Objectives	Availability, stability and integrity of the AD infrastructure must be maintained. Must secure the core components of the AD by implementing appropriate group policies for Domains and Domain Controllers.

Risk 1.8	Unused/unnecessary services not disabled on the AD servers/Domain Controllers.
Probability	High
Impact	Services that are installed by default but rarely used can contain widely exploited flaws that will put the Domain Controllers at risk.
Priority	Critical
Control Objectives	System integrity and availability must be maintained. Some services that have known security issues like, IIS, RAS and Terminal Services, must be carefully configured by skilled Administrators.

Risk 1.9	Failure of the DNS
Probability	High
Impact	The AD service will fail to locate network resources.
Priority	Critical
Control Objectives	The loss of the DNS must be prevented because it is used by the AD to locate services on other hosts that network users may rely on. The security design must ensure that a single point of failure does not happen.

Risk 1.10	Responsibilities for the management of GPOs not clearly defined. Changes to group policies not implemented in a controlled manner.
Probability	High
Impact	Group policies that are incorrectly configured and applied could open up security holes to the AD and the internal network. For example, allowing anonymous logon and having passwords that never expire, allowing Everyone/Full Control access permissions on file shares, and having unnecessary members in the Administrators and Guest user groups. Group policy changes that are not properly managed can produce unexpected results in the user environment, and affect the integrity and availability of the AD infrastructure. They also make troubleshooting difficult.
Priority	Critical
Control Objectives	Availability, stability and integrity of the AD infrastructure must be maintained. The ability to modify group policies must be restricted to a limited number of administrators.

	Changes to the group policies must follow the Change Control Management process.

Risk 1.11	Unauthorized access to proprietary network and directory services details on Domain Controllers, which do not have screen saver turned on, when left unattended.
Probability	Medium
Impact	Potential loss of system availability and integrity, and unauthorised access to confidential corporate data. Also potential loss of credibility.
Priority	Critical
Control Objectives	Disclosure of proprietary information must be minimized. Screen saver must be password protected, and activated after 3 minutes of inactivity on the Domain Controllers.

Risk 1.12	Organisational units (OUs) not protected and not regularly monitored.
Probability	High
Impact	Incorrectly configured OUs will result in inappropriate inheritance of policies by the OUs as well as the user and computer objects within the OUs. Without regular monitoring, intrusion could happen without being detected and dealt with in a timely manner.
Priority	Critical
Control Objectives	OUs must have the right permissions assigned. Unknown OU objects that were not created by the administrators must be detected and removed.

Risk 1.13	Inappropriate Domain Trusts
Probability	High
Impact	Potential problems caused by remote administrators, made possible by two-way transitive trust between the forest root and the parent domain and the child domain.
Priority	Critical
Control Objectives	Potential security breaches and corruptions caused by remote administrators must be minimized. The need to have two-way transitive trust must be carefully reviewed.

Risk 1.14	GPOs not documented.
Probability	High
Impact	In the situation of an AD catastrophe, a full recovery of group policies, which contain over 600 policy settings, may not be possible. It would also be difficult to troubleshoot policy related problems if GPOs are not fully documented.
Priority	Critical

Control Objectives	The integrity and availability of the AD must be maintained. The design of the AD and GPOs settings must be fully documented.

Risk 1.15	The Guest account is not disabled.
Probability	Low
Impact	Misuse of services that have inadvertently left open using the Guest account, which allows anonymous access to computer.
Priority	Medium
Control Objectives	Appropriate authentication and authorized access to the system must be maintained.

Risk 1.16	The Administrator account is not renamed.
Probability	High
Impact	Since the 'Administrator' username cannot be locked out, hackers can try as many times as they like to hack and crack its password. After finding the 'Administrator' username and having obtained its password, hackers can then use it to hack other local accounts. If the hacking activity is successful, it will compromise the security of the AD infrastructure, affecting its integrity and availability.
Priority	Critical
Control Objectives	The integrity and availability of the AD must be maintained.

Risk 1.17	Anonymous user not disabled.
Probability	High
Impact	Potential unauthorized access because anonymous users can enumerate the names of domain accounts and network shares. Malicious users could take advantage of this vulnerability to obtain critical information pertaining to an internal network, and launch an attack or gain unauthorized access.
Priority	Critical
Control Objectives	Anonymous users must be disallowed, to insure the confidentiality and availability of the AD are maintained.

Risk 1.18	Drives are not formatted NTFS
Probability	Low
Impact	Domain controllers and large drives require NTFS. Lack of reliability and security with the FAT and FAT32 file systems.
Priority	Critical
Control Objectives	The reliability, security and availability of the AD domain must be maintained.

Risk 1.19	Inactive and redundant accounts not disabled or deleted. Unnecessary file shares not removed.
Probability	High
Impact	Potential exposure to unauthorized access to the system, making use of inactive or redundant accounts, and the redundant file shares. In addition, accounts having 'admin' permissions can be used to further exploit any known vulnerabilities within the AD infrastructure.
Priority	Medium
Control Objectives	Confidentiality, integrity and availability of the AD infrastructure must be maintained. Must minimize the exposure to risk of unauthorised access to the system, by malicious users who leverage the redundant accounts and file shares as entries to the local system.

Risk 1.20	Auditing not enabled and system administrators not analysing log files regularly.
Probability	High
Impact	Unauthorized access and malicious activities could occur on the AD without being logged or detected.
Priority	Critical
Control Objectives	The confidentiality, integrity and availability of the AD must be maintained. Subsequently, auditing must be enabled on domain controllers, servers and computers. This can be managed efficiently with group policies on the various OUs containing the domain controllers, servers or computers.

Risk 1.21	Administrators use single logon accounts for everything, including non-administrative tasks, for example, running Office applications and reading e-mail.
Probability	High
Impact	If an attack is successful, an intruder could leverage the 'admin' privileges of the administrators, and the damage to the AD infrastructure could be a catastrophe.
Priority	Critical
Control Objectives	Confidentiality, integrity, availability and credibility of the network must be maintained. Administrators must have one regular account for running non-administrative programs, and at least one other account for administrative tasks.

Risk 1.22	Domain master roles not secured
Probability	High
Impact	Failure to write to directory schema. Failure to add or remove domains.

Priority	Critical
Control Objectives	To maintain the integrity and availability of the AD, the schema master must be protected because only this domain controller can write to the directory schema.

Risk 1.23	Reading of email on the AD servers (or any server)
Probability	Medium
Impact	Potential of a denial of service attack from email virus, or executable attachment containing malicious code
Priority	Critical
Control Objectives	The loss of system availability and business productivity must be minimized. Apart from the email client, applications and utilities that are not strictly required by the server must not be installed.

Internal Processes, Policies and Procedures

Risk 1.24	Antivirus software not installed and virus signatures not up-to-date
Probability	Medium
Impact	The lack of antivirus software or outdated virus signatures can compromise the security of the system, against malicious code, virus and Trojan horses.
Priority	Critical
Control Objectives	System corruption and disruption to operations/loss of productivity, as a result of a virus attack, must be minimized

Risk 1.25	The AD database and GPOs not backed up and restore not tested.
Probability	High
Impact	High impact on the availability of the AD and GPOs. In worst cases, it could take days or weeks to restore the entire AD. It would also be extremely time-consuming to recreate GPOs, especially if not documented. Without appropriate GPOs the integrity of the AD infrastructure could be compromised.
Priority	Critical
Control Objectives	Availability and integrity of the AD infrastructure must be maintained. Backups of the AD database and all the respective domain controllers, and GPO(s) must be tested to verify that a restore is possible from the backup.

Risk 1.26	The AD servers are not physically secured
Probability	Medium

Impact	Apart from potential physical damage to the servers, there is also exposure to unauthorised access to proprietary information
Priority	Critical
Control Objectives	System integrity and availability must be maintained. Warranty from vendor must not be void; resulting in financial loss, confidentiality of intellectual information must be maintained.

Risk 1.27	Change Control Management procedures not followed or inadequate change control
Probability	Medium
Impact	Potential system downtime caused by incorrect or inadvertent settings to a group policy at the top level of the AD
Priority	Critical
Control Objectives	Integrity of the AD domain and its availability must be maintained.

Current State of Practice

In my opinion, there are sufficient resources to create and conduct a comprehensive audit for Windows 2000 AD. There are two main sources of references that I used, one is public information and two is proprietary information from *The Company* itself.

For public information I used the common Internet search engines for performing my research, especially Google. In addition, I did a thorough search of vulnerability, checklist and tools repositories for the system I am auditing. I have found Whitepapers from some vendors an extremely good source of information.

To obtain proprietary information I had to work with the key personnel who are responsible for the installation, configuration and administration of the Windows 2000 AD. *The Company*'s Windows 2000/AD Architecture Detailed Design document was reviewed to discover any security flaws with the original design. Internal processes, policies and procedures that may impact the security of the Windows 2000 AD were also reviewed to discover any inadequacy or finetuning required.

A full list of references used to research on AD security is provided in Appendix A, with the exception of the proprietary information. Of all the research references used, the following are particularly useful for my audit exercise:

- SANS Reading Room
  http://rr.sans.org
- Securing Windows 2000 Active Directory (Part 1 - 4)
  http://www.windowsecurity.com/articles/windows_os_security/
- Windows 2000 Security Checklist
  http://www.labmice.net/articles/securingwin2000.htm
- Windows 2000 Server Baseline Security Checklist
  http://w2kinfo.nacs.uci.edu/Member_server_baseline_sec.htm
- Securely Managing Your Group Policies. White Paper
  http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolici
  es.pdf
- Basic Security Issues of Active Directory
  http://www.sans.org/rr/win2000/active_dir.php
- Advanced Security Management of Active Directory in Windows 2000
  http://www.quest.com/whitepapers/Quest-HP_AD_Security_WPFinal.pdf
- Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I, Version 1.0
  http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=
  F937A913-F26E-49B5-A21E-20BA5930238D (download link)

Assignment 2 – Create an Audit Checklist

The checklist is divided into two sections:
- ***Active Directory (AD) Security***
- ***Internal Processes, Policies and Procedures***
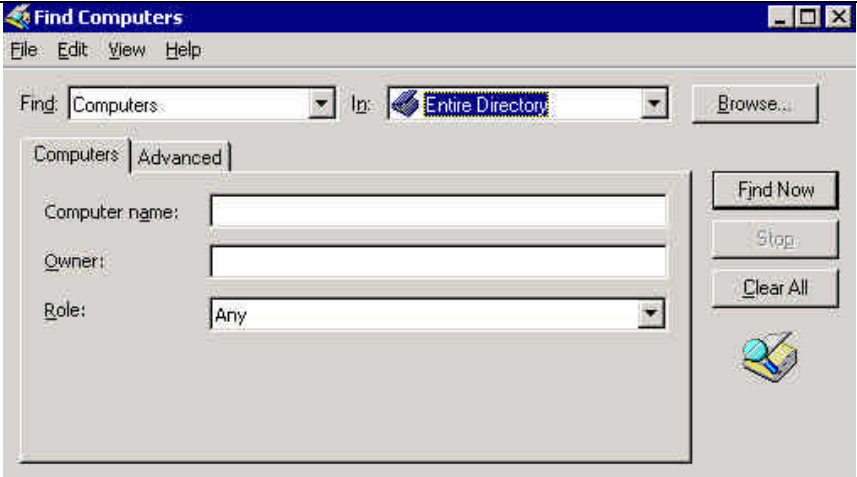
NOTE: All system testing must be performed using an account with sufficient 'admin' permissions to the AD Domain Controllers. This requires the auditor to work closely with a system administrator, whose availability must be ascertained before the audit begins. Alternatively, the auditor can be provided with a 'system admin' equivalent logon account for the duration of the audit, with just sufficient permissions for completing the audit. The second option is assumed to be the case in this assignment.

Active Directory (AD) Security

Check #1 – Domain Controllers

Reference	• Magalhaes, Ricky M. Securing Windows 2000 Active Directory (Part 2). 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows _2000_Active_Directory_Part_2.html
Control objective	Since Domain controllers contain sensitive data used for authentication, its availability must be maintained at all time. Domain controllers must be physically secured. Access to the Domain controllers must be restricted to a small group of authorized and skilled personnel.
Risk	Inadequate protection for the Domain Controllers.
Likelihood	High
Consequence	Failure of a domain controller, especially if fault tolerance does not exist, will stop domain authentication from working.
Compliance/ Expected Results	• For redundancy, more than one domain controllers exist in the Root Domain and Child Domains. • Domain controllers are physically secured in computer rooms where access is tightly controlled. • A current Computer Room Access Policy is in place.
Testing	1) From the auditor workstation run 'Active Directory Users and Computers'. 2) Right-click on the domain to be audited, and select 'Find…' 3) In the 'Find' selection box, select 'Computers'. 4) In the 'In' selection box, select 'Entire Directory' (or select the Root Domain followed by the individual Child Domain). 5) Click 'Find Now' to continue.
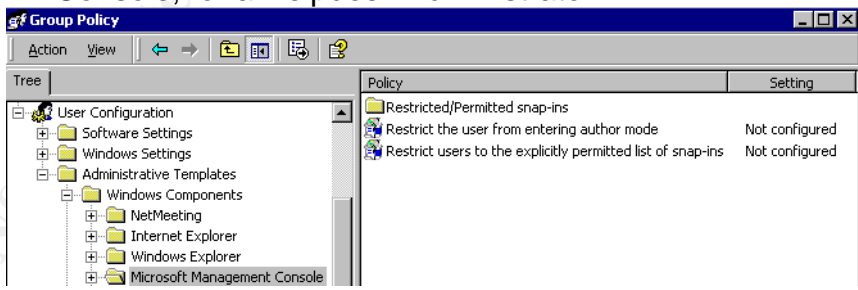
6) In the display pane of the 'Find Computers' window, click the 'Machine Role' column header, to sort the computers by type.

7) Gather evidence that multiple computers are listed as having the 'Domain Controller' machine role.
8) Gather evidence of a current and adequate Computer Room Access Policy.
9) Document the findings in the audit report.

Objective/ Subjective	Objective

Check #2 – Delegating Administrative Control of the AD Objects

Reference	• netiQ. Securely Managing Your Group Policies. White Paper, 11 March 2002. http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf • Internal documentation of administrative roles and responsibilities for the AD
Control objective	Integrity of the AD and its availability must be maintained. Administrative roles and responsibilities must be clearly defined. The ability of individuals to perform certain AD administrative functions must be appropriately controlled. Unauthorised access to information in the AD must be minimized.
Risk	Lack of clearly defined roles and responsibilities for the administration of the AD, and inappropriate delegation of administrative control for the AD objects.
Likelihood	High
Consequence	Poor management and unauthorised access to the AD infrastructure, which could have high impact on the availability of the AD. The end result would be a lack of accountability for changes occurred and ownership for problems resolution, resulting in poor service delivery to the users.
Compliance/ Expected Results	1) Roles and responsibilities for the administration of the AD are clearly defined and documented. 2) The roles of Schema Admin, Enterprise Admin, Domain Admin, Backup Operators and Server Operators, are assigned to system administrators, based on their roles and responsibilities for the AD. Hence different levels of administrators have different delegated authorities over different parts of the AD. For example, a Helpdesk Administrator who is tasked with the 'Password Reset' and 'Unlock User Account' administrative role will be granted with appropriate permissions on only the user objects. The Helpdesk Administrator will not have the authority to manage computer objects, which is a task of the technicians or system administrators.
Testing	1) From the auditor workstation, run 'Active Directory Users and Computers'. 2) Select the domain node to be audited. 3) Right-click on the domain OU and select Properties. 4) From the *domain* Properties window select 'Security'.

	5) Click the 'Advanced…' button to view additional permissions.
	6) From the Access Control Settings for *<domain>* window, select the 'Permissions' tab (by default).
	7) From the list of permission entries, locate entries that are related to 'User Access Specialist', who are responsible for the maintenance of user accounts and groups.
	8) Make sure the 'User Access Specialist' administrative role is only granted specific permissions for the management of user and user group objects.
	9) Click 'Cancel' a couple of times to close the open windows.
	Stimulus/Response Testing:
	1) Request one of the User Access Specialists to logon to the domain to be audited.
	2) Run Active Directory Users and Computers.
	3) Expand the domain node.
	4) Right-click on an OU.
	5) Select New.
	6) Confirm that only the 'User' object is available.
	7) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective

Check #3 – MMC Consoles

Reference	• Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 2)". 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_2.html • Internal documentation of administrative roles and responsibilities for the AD.
Control objective	The integrity and availability of the AD must be maintained. The risk of an intruder gaining full control of the admin tools must be minimized. Access to MMC snap-ins must be restricted based on the roles and responsibilities for the AD.
Risk	Access to MMC consoles not restricted, and not inline with the AD administrative roles and responsibilities.
Likelihood	Medium
Consequence	If delegation of administration is lacking or incorrectly configured, an intruder with full control of the admin tools could exploit the admin privileges to gain unauthorized access to critical information in the AD.
Compliance/ Expected Results	• Permissions to run specific administrative tools are mapped to administrative authorities that have been delegated to a user for an administrative task. • For further security, users can be prevented from running MMC console in author mode.
Testing	1) Request the system administrator to provide screenshots of GPO settings for Microsoft Management Console, for a Helpdesk Administrator. 2) For the Restricted/Permitted snap-ins policies, verify that admin snap-ins, especially 'Active Directory Domains and Trusts', 'Active Directory Sites and Services', 'Security Configuration and Analysis', and 'Security Templates' are restricted from the Helpdesk Administrator. Depending on the environment, some other snap-ins could be restricted too.

3) Depending on the environment, the 'Restrict the user from entering author mode' policy could be enabled to provide further security.

Stimulus/Response Testing:
1) From the Helpdesk Administrator's workstation, click Start | Run.
2) Enter 'mmc' and press Enter.
3) From the Console menu confirm that the Add/Remove Snap-in… option is not available.

4) From the Console menu, select 'Add/Remove Snap-in'.
5) On the 'Add/Remove Snap-in' window, click Add. The 'Add Standalone Snap-in' window will be displayed.

	6) Confirm that all the restricted snap-ins do not appear in the list of Available Standalone Snap-ins. 7) Click on Close to close the 'Add Standalone Snap-in' window. 8) Click Cancel to close the 'Add/Remove Snap-in' window. 9) Document findings in audit report.
Objective/ Subjective	Objective

Check #4 – AD Access Controls and ACLs

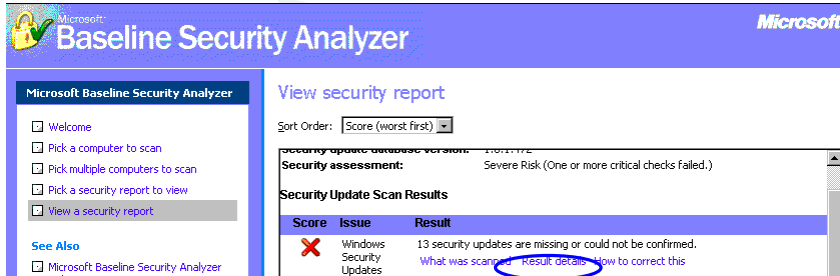|	
Reference	• Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I. Version 1.0 (*Table 11*) http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link) • Microsoft Baseline Security Analyzer http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link)
Control objective	Unauthorised access to system files and executables, file shares and registry keys must be minimized. The risk of disk-space attacks on AD domain controllers must be minimised. Appropriate ACLs must be applied to registry keys, file system and other data (and log) partitions; in order to maintain the stability and integrity of the AD infrastructure.
Risk	Default AD access permissions and NTFS ACLs are too permissive, granting **Everyone** group **Full Control** permissions on the root of each logical disk volume on the AD, and newly created file shares and registry keys.
Likelihood	High
Consequence	Vulnerability of domain controller to disk-space attacks on each disk volume, including the AD database files volume. Inappropriate access permissions assigned to file shares and registry keys.
Compliance/ Expected Results	• 'Everyone – Full Control' permission is not granted to the root of each logical disk volume. • Files and folders on the domain controllers are appropriately secured, as shown in following table. <table><tr><th>File or Folder</th><th>Permissions</th></tr><tr><td>Root of each logical disk volume</td><td>1. Allow Read and Execute for Everyone 2. Allow Full Control for Administrators</td></tr></table> • Default ACL permissions on file shares, file system and registry keys in GPOs modified, with 'Authenticated Users'/Appropriate access control replacing 'Everyone/Full Control' permissions.
Testing	<u>AD Access Controls</u> 1) From the auditor workstation, run 'Computer Management'

2) Right-click on 'Computer Management (Local)' and
   select 'Connect to another computer …'.
3) Select a domain controller from the AD and click OK.
4) Expand the 'Storage' node.
5) Click 'Disk Management'.
6) Right-click on the 'root volume', that is, 'C:', and select
   'Properties'.
7) On the 'Local Disk (C:) Properties' screen, select the
   'Security' tab.

	8) Verify that appropriate permissions have been assigned to each user or user group for the root of all logical disk volumes. <u>ACLs</u> 9) Down and install MBSA. 10) Run MBSA and scan the AD domain controllers. 11) From MBSA | View Security Report, locate the 'Additional System Information' section. 12) Select 'Result Details' for the 'Shares' issue. 13) Verify that appropriate access permissions are assigned to the shares and in particular, 'Everyone' is not granted Full Access to any of the shares. 14) Document findings in the audit report.
Objective/ Subjective	Objective

Check #5 – Service Packs and Hotfixes

Reference	• Internal documentation on Service Packs and Hotfixes implementation process and schedule. • Microsoft Baseline Security Analyzer http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link)
Control objective	Exposure to published security threats must be minimized, by the timely implementation of Service Packs and hotfixes.
Risk	Domain Controllers not kept up-to-date with the latest Service Pack and security Hotfixes.
Likelihood	High
Consequence	Exposure to known security threats, through unauthorised access to the system, with elevated privileges at the server level.
Compliance/ Expected Results	• No security updates are reported missing.
Testing	1) Under the 'Security Update Scan Results' section, check the score and result for the 'Windows Security Updates' item. 2) If there are missing security updates, click on the 'Result details' link for further details. 3) Document the findings in the audit report.
Objective/ Subjective	Objective

Check #6 – Password Security

Reference	• Internal policy document on logon account and password. • "Windows 2000 Security Checklist" http://www.labmice.net/articles/securingwin2000.htm (item 8) • @stake LC4 password auditing and recovery application http://stake.com/research/lc/download.html (download link) • pwdump3 Windows NT/2000 remote password hash grabber http://www.polivec.com/pwdumpdownload.html (download link)
Control objective	Must have strong password policy in place. Systems must be configured to force all passwords to meet the complexity requirements. To enhance security, different passwords should be used on each server in a workgroup or domain. The Administrator account password must contain at least one non-alphanumeric character in the first seven characters.
Risk	Inadequate account and password policies, permitting the use of weak passwords. Weak passwords are easy to guess, simple to derive, and vulnerable to dictionary attack. Password hacking freeware are readily available that will do the job for the hackers, making a denial of service attack possible or gaining unauthorized access to proprietary information.
Likelihood	High
Consequence	Potential loss of system availability and integrity, should the compromised account have privileged permissions to the network. Unauthorised access to confidential corporate data.
Compliance/ Expected Results	• Password length must be set to at least 8 characters long, must expire at least every 60 days, must enforce password history, and password complexity requirements must be enabled. By default, all these settings are not defined. • To complement the system settings, a current internal logon account and password policy is in place.
Testing	1) From the auditor workstation, create an audit MMC. Click Start | Run, enter mmc and click OK. 2) From the Console menu, select 'Add/Remove Snap-in'. 3) From the list of available Standalone Snap-ins, select

‘Security Configuration and Analysis’ and click Add.
4) Repeat steps 2-3 for adding the Security Templates snap-in.
5) Click OK to close the ‘Add/Remove Snap-in’ window.

6) Expand the ‘Security Templates’ node to display all the templates within.
7) Highlight the ‘basicwk’ security template, select ‘Action | Save As’ and name the new template ‘audit’.
8) Expand the ‘audit’ template and Account Policies node.
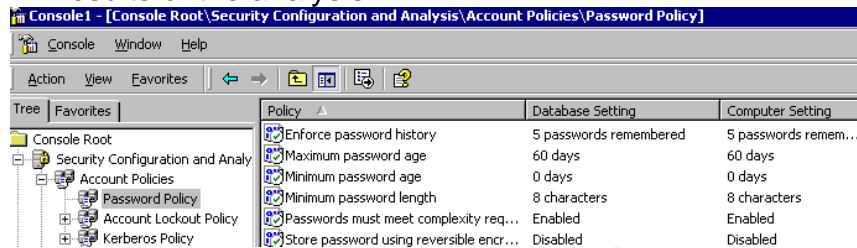9) Select the ‘Password Policy’ node.

Modify the password policies as follow.
10) Set Enforce password history to 5 passwords remembered.
11) Set Maximum password age to 60 days
12) Set Minimum password age to 1 days
13) Set Minimum password length to 8 characters
14) Enable ‘Passwords must meet complexity requirements’
15) Highlight the ‘audit’ template, select Action | Save As to re-save the ‘audit’ template with the changes made.
16) Right-click the ‘Security Configuration and Analysis’ scope item, and select Open Database.
17) Save the database as ‘audit.sdb’.
18) Click Open
19) Right-click the ‘Security Configuration and Analysis’ scope item again, and select ‘Import Template…’.
20) From the Import Template window, select the ‘audit.inf’ template and click Open to import the template into the database.

<table>
<tr>
<td></td>
<td>

21) From the Action menu, select Analyze Computer Now. Accept the default location for the log file.

22) Once the analysis is finished, expand the 'Security Configuration and Analysis' scope item to view the results of the analysis.

23) Look for red X's, which are system settings that deviate from the database settings.

24) From the Console menu, select 'Save' and name it 'audit.msc'. Close the MMC console.

25) For convenience of future use, send a shortcut of the file to the desktop.

26) Document the findings and attach screenshots to the report.

27) Further test can be done to discover all weak passwords on the domain, using a combination of the LC4 password auditing and pwdump3 password hash grabber tools. Both tools need to be downloaded and files extracted/installed beforehand.

28) From the auditor's workstation:

- From the command prompt, from the pwdump3 program folder, run "pwpump3 <machinename of domain controller> <output filename>"
- run LC4, and from the 'Get Encrypted Password' screen, select 'Retrieve from a remote machine'
- click Next
- choose the 'Custom' auditing method
- click the 'Custom Options…' button

</td>
</tr>
</table>

Sylvia Choa GSNA Practical Assignment v2.1

- select the top two options,
- ensure the 'brute force attack' option is not selected, as it is not required for this audit
- click OK to continue
- accept the default 'Pick Reporting Style' settings and click Next to continue
- click Finish to continue
- at the 'Import From Remote Registry' screen, click Cancel to continue

- click OK at the warning message
- From the Import menu select 'Import From PWDUMP File' and specify the output filename generated from running pwpump3.

- From the Session menu select 'Begin Audit'. It might take a while (5 minutes or more), depending on the number of user accounts in the domain that's being audited.
- On completion, from the File menu export the session to a text file for further analysis.

Stimulus/Response Test:
1) From the auditor's workstation, press Ctrl+Alt+Del.
2) Select Change Password….
3) Enter the old password followed by the new password and click OK.
   - For the new password, first enter '+Abc4' as the new password, which satisfies the complexity requirement but fails the minimum length requirement.
   - Secondly, enter 'abc4567890' as the new password, which satisfies the minimum length requirement but fails the complexity requirement.
   - In both cases, assuming the minimum length policy is set to 8, the following error message will be displayed.

   - Thirdly, enter '(S4v4nw0nd4rs)' as the new password (assuming this password has not been used during recent time), which satisfies all three requirements of password history, length and complexity. The system should accept it as a valid password.
4) Gather evidence of a current internal logon account and password policy.
5) Attach screenshot and document findings in audit report.

| Objective/ | Objective |

Subjective	

Check #7 – GPOs for Securing the Domains and Domain Controllers

Reference	• Internal documentation on group policies for Domains, Domain Controllers. • Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I. Version 1.0. (Chapter 4, *Tables 12-16, 29-30*) http://www.microsoft.com/downloads/details.aspx?displayla ng=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link)
Control objective	Availability, stability and integrity of the AD infrastructure must be maintained. Must secure the core components of the AD by implementing appropriate group policies for Domains and Domain Controllers.
Risk	The core components of the AD are not protected from unauthorised access.
Likelihood	High
Consequence	Adverse impact on the stability, integrity and availability of the AD.
Compliance/ Expected Results	• Appropriate group policies have been implemented for the Domains in the following categories of policy settings: (1) password policy, (2) account lockout policy and (3) Kerberos policy. • Appropriate group policies have been implemented for Domain Controllers in the following categories of policy settings: (1) audit policy, (2) user rights assignment, (3) security options, and (4) event log.
Testing	1) Assume you have completed Check #6. 2) From the auditor workstation, open the 'audit.msc' MMC created in Check #6. Domains 3) Highlight the 'Security Templates' and expand the 'audit' node. 4) Apply best practice policy settings to Account Policies -

Password Policy, Account Lockout Policy, and Kerberos Policy.

5) Right-click on the 'audit' template and select 'Save As…' to re-save the 'audit' template.
6) Right-click the 'Security Configuration and Analysis' scope item, and select 'Import Template…'.
7) From the Import Template window, select the template that you have saved in step (6), i.e., 'Domain audit.inf'.
8) Click Open to import the template into the database.
9) From the Action menu, select Analyze Computer Now. Accept the default location for the log file.
10) Once the analysis is finished, expand the 'Security Configuration and Analysis' scope item to view the results of the analysis.

11) Expand each category of policy under 'Account Policies'.
12) Look for red X's, which are system settings that deviate from the database settings.
13) From the Console menu, select 'Save' to re-save the 'audit.msc' console.

Domain Controllers (complete this test in conjunction with the system administrator)
1) From the auditor/administrator workstation run 'Active Directory Users and Computers'.
2) Right-click the Domain Controllers OU.
3) Select 'Properties'.
4) Select the 'Group Policy' tab.

5) With the 'Default Domain Controllers Policy' highlighted, click 'Edit'.
6) Expand 'Computer Configuration | Windows Settings | Security Settings | Local Policies'.
7) Verify that the settings for 'Audit Policy', 'User Rights Assignment' (particularly 'Log on locally' and 'Shut down the system' policies), and 'Security Options' conform to best practice settings for Domain Controllers.
8) Repeat step (7) for 'Event Log | Settings for Event Logs'.

9) Document the findings and attach screenshots to the

	report.
	Stimulus/Response Test: <u>Domains</u> 1) Check #6 is one of the tests for the Domain policies. Another test could be completed on the 'Account Lockout Policy' using an account provided by the system administrator. Verify that the account gets locked out after a number of failed logon attempts, using a wrong password. <u>Domain Controllers</u> 2) Working in conjunction with the system administrator, verify that a general user account cannot log on locally to the Domain Controller. 3) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective

Check #8 – Services

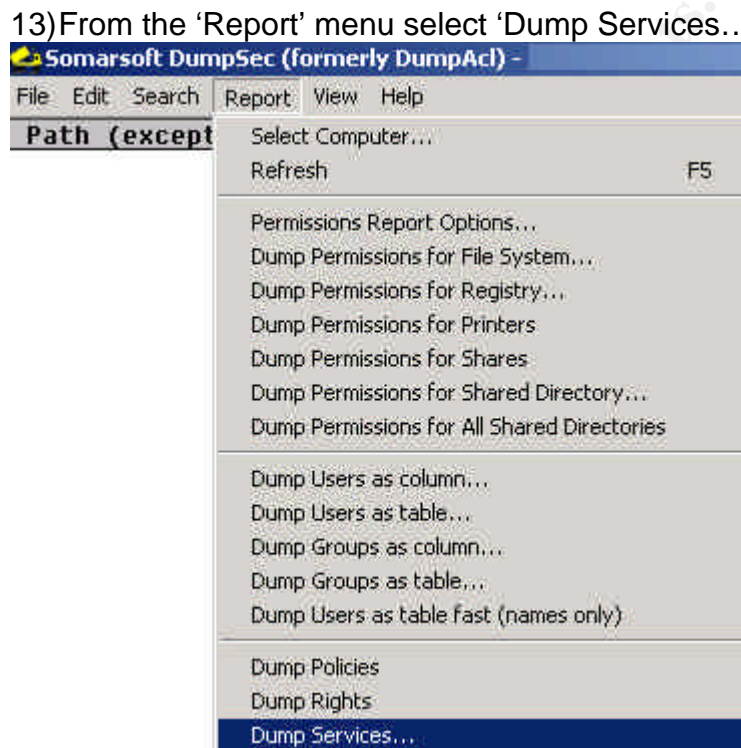| Reference	• Microsoft Baseline Security Analyzer (MBSA) http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link) • Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I. Version 1.0. (Chapter 3, *Table 9*) http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link) • SomarSoft Utilities. DumpSec http://www.somarsoft.com/ (download link)
Control objective	System integrity and availability must be maintained. Some services that have known security issues like, IIS, RAS and Terminal Services, must be reviewed and carefully configured. Network services that are not required for the server role must be disabled, in particular, the IIS components.
Risk	Unused/unnecessary services not disabled on the AD servers.
Likelihood	High
Consequence	Services that are installed by default but rarely used can contain widely exploited flaws that will put the operating system at risk.
Compliance/ Expected Results	Unnecessary services are disabled on the Domain Controllers. Common services to disable on Domain Controllers are: • Application Manager • ClipBook • Distributed Link Tracking • Distributed Transaction Coordinator • Fax Service • FTP Publishing Service (unless using for web hosting) • Indexing Service • IIS Admin Service (unless using for web hosting) • Internet Connection Sharing • License Logging Service • NetMeeting Remote Desktop Sharing • Print Spooler • QoS RSVP • Remote Access Auto Connection Manager • Remote Access Connection Manager

	• Routing and Remote Access • Telephony • Telnet • Utility Manager
Testing	1) Download and install MBSA. 2) Run MBSA to scan the AD servers. 3) From the security report locate the Additional System Information section. 4) For the 'Services' issue, click 'Result details'. **Additional System Information** 	Score	Issue	Result
---	---	---
✳	Auditing	Logon Success and Logon Failure auditing are both enabled. What was scanned

✳	Services	Some potentially unnecessary services are installed.
		What was scanned Result details How to correct this |
		
		5) By default, this only scan for the following services, but the configurable list of services to be checked can be modified:
		    MSFTPSVC (FTP)
		    TlntSvr (Telnet)
		    W3SVC (WWW)
		    SMTPSVC (SMTP)
		
		6) Investigate the list of potentially unnecessary services that are installed on the AD servers. They should be disabled.
		
		Microsoft Baseline Security Analyzer - Microsoft Internet Explorer provided by
		
		Baseline Security Analyzer
		
		Some potentially unnecessary services are installed.
		
		Result Details
		
		The following list of services should only be enabled on computers that require their functionality. Services that are not required should be disabled to reduce the attack surface of the system.
		
		| Score
			Service	State

---	---	---
✳	Telnet	Stopped	 7) Attach screenshots and document findings in the audit report. 8) Use the SomarSoft DumpSec utility to obtain a complete list of services installed on the servers. 9) Download and install the SomarSoft DumpSec utility. 10) Run DumpSec from the auditor workstation.

11) From the 'Report' menu select 'Select Computer…'.

Somarsoft DumpSec (formerly DumpAcl) -
File Edit Search Report View Help
Path (except Select Computer…
                  Refresh   F5

12) Enter the name of the Domain Controller to be audited and click OK.

13) From the 'Report' menu select 'Dump Services…'.

Somarsoft DumpSec (formerly DumpAcl) -
File Edit Search Report View Help
Path (except Select Computer…
                  Refresh   F5

                  Permissions Report Options…
                  Dump Permissions for File System…
                  Dump Permissions for Registry…
                  Dump Permissions for Printers
                  Dump Permissions for Shares
                  Dump Permissions for Shared Directory…
                  Dump Permissions for All Shared Directories

                  Dump Users as column…
                  Dump Users as table…
                  Dump Groups as column…
                  Dump Groups as table…
                  Dump Users as table fast (names only)

                  Dump Policies
                  Dump Rights
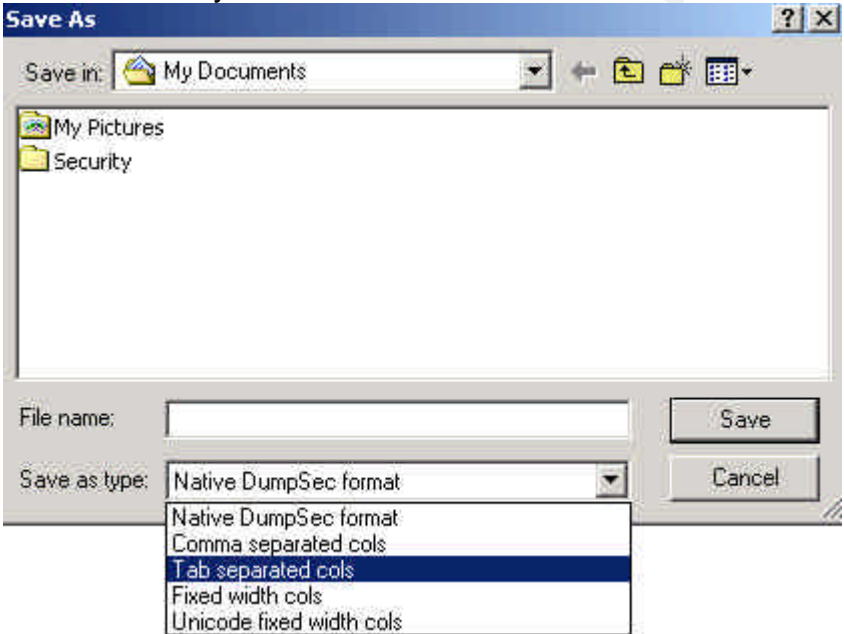   Dump Services…

14) On the 'Options for Services/Drivers Report' screen uncheck the 'Kernel drivers' selection box.

Options for Services/Drivers Report
Type
  ☑ Win32 Services
  ☐ Kernel drivers
Status
  ☑ Running
  ☑ Not Running

  OK   Cancel

15) Click OK to continue.
16) On completion, click File | Save Report As…

Somarsoft DumpSec (formerly Du

File Edit Search Report View Help

Save Report As...   Ctrl+S
Load Native File...
Load Multiple Native Files...

17) Save the output file to an appropriate file type, this can then be imported into a spreadsheet or database for further analysis.

Save As

Save in: My Documents

My Pictures
Security

File name:

Save as type: Native DumpSec format

Native DumpSec format
Comma separated cols
Tab separated cols
Fixed width cols
Unicode fixed width cols

Save

Cancel

18) Analyze the output file for unnecessary services for the Domain Controller role.
19) Document the findings in the audit report.
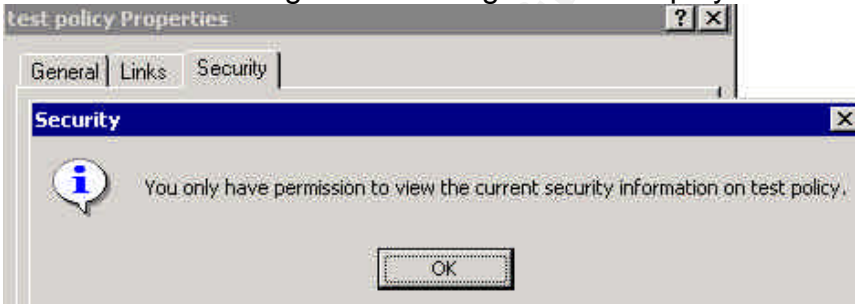
Objective/ Subjective	Objective

Check #9 – DNS

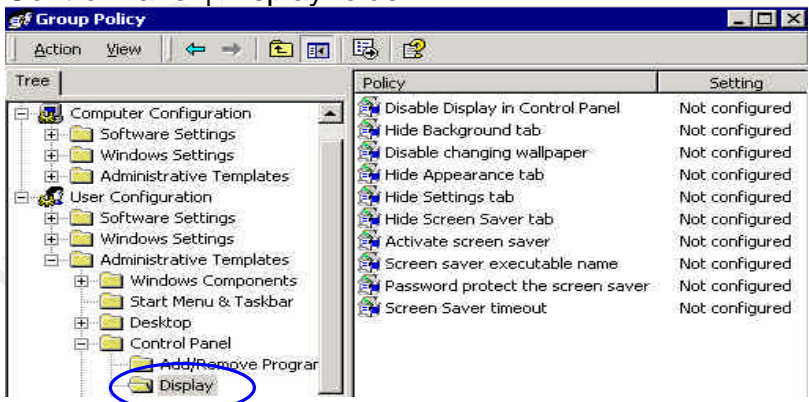| Reference	• Microsoft. Security Operations Guide for Windows 2000 Server. Chapter 3 - Managing Security with Windows 2000 Group Policy http://www.microsoft.com/downloads/details.aspx?FamilyID=f0b7b4ee-201a-4b40-a0d2-cdd9775aeff8&DisplayLang=en (download link) • DcDiag.exe: Domain Controller Diagnostic Tool, • NetDiag.exe: Network Connectivity Tester, From Microsoft Windows 2000 SP3 Support Tools http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/supporttools.asp (download link)
Control objective	The loss of the DNS must be prevented because it is used by the AD to locate services on other hosts that network users may rely on. Must prevent unauthorized users from exploiting it as a means of gaining access to the AD.
Risk	Failure of the DNS
Likelihood	High
Consequence	The AD service will fail to locate network resources.
Compliance/ Expected Results	No errors should be reported from the running of the Windows 2000 SP3 Support Tools: dcdiag and netdiag.

Testing	1) Perform this test in conjunction with the system administrator.
	2) Install the Windows 2000 SP3 Support Tools.
	3) Provide the system administrator with a floppy disk (or CD) containing DcDiag.exe and NetDiag.exe.
	4) Run the tools on each Domain Controller in each Domain or have a batch file for scanning all the Domain Controllers in each Domain. Both tools are to be run from the command prompt.
	5) The command line for DcDiag.exe is:
	  • Dcdiag */s:DomainController* /u:*Domain\UserName* /p:* /f:*outputfilename.Log*
	  • (username is the user account of the administrator)
	6) The command line for NetDiag.exe is:
	  • Netdiag /d:*DomainName* > *outputfilename.Log*
	7) If there are errors found in the output files, rerun the same commands with the additional /v (verbose) flag to generate output with extended information.
	8) Document the findings in the report.

Objective/ Subjective	Objective

Check #10 – GPOs Security

Reference	• netiQ. Securely Managing Your Group Policies. White Paper, 11 March 2002. http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf
Control objective	Availability, stability and integrity of the AD infrastructure must be maintained. The ability to modify group policies must be restricted to a limited number of administrators. Changes to the group policies must follow the Change Control Management process. Must be able to back up and restore all or selective GPOs. To enhance security and provide redundancy for quick disaster recovery, offline storage of policy settings through templates must be considered.
Risk	Responsibilities for the management of GPOs not clearly defined. By default, all 'Domain Admins' of a child domain can modify group policies within that domain. And, some backup software runs as a Windows 2000 Service and needs to be a member of 'Domain Admins' for it to work. Such service accounts, once their passwords are discovered, are an alternative source for gaining unauthorised access to the GPOs. Changes to group policies not implemented in a controlled manner. GPOs and/or system state of all AD Domain Controllers not backed up and restore not tested.
Likelihood	High
Consequence	Group policies that are incorrectly configured and applied could open up security holes to the AD and the internal network. For example, allowing anonymous logon and having passwords that never expire, allowing Everyone/Full Control access permissions on file shares, and having unnecessary members in the Administrators and Guest user groups. Group policy changes that are not properly managed can produce unexpected results in the user environment, and affect the integrity and availability of the AD infrastructure. They also make troubleshooting difficult. Using the default settings, the larger the number of 'Domain Admins', the more difficult it is to establish accountability for group policy changes, and maintain the integrity and stability of the AD. Disaster recovery is impossible without successful backup

	of the AD Domain Controllers and GPOs.

Compliance/ Expected Results	• Responsibilities for the GPOs are clearly defined and understood by the system and security administrators.
	• Change Control Management procedures are followed for changes made to the group policies.
	• Restrictions have been applied to GPOs to allow only specific administrators the ability to 'edit' the GPOs. For example, only the 'Enterprise Admins' are allowed to modify group policies, and the 'Domain Admins' are denied the following permissions on all or selected GPOs and the OU that contains the GPOs.
	  ▪ Write
	  ▪ Create All Child Objects
	  ▪ Delete All Child Objects
	This is particularly useful when the 'Domain Admins' user group contains a wide range of user accounts, including service accounts of server backup software, for example, that are running on the AD Domain Controllers.
	
	It is advisable to centralize the GPOs in an OU.

Testing	1) Gather evidence that the responsibilities for the GPOs are clearly defined and understood by the system and security administrators. This can be achieved by acquiring the necessary documentation relating to the AD infrastructure, roles and responsibilities for AD, and interviewing key security and/or system administrators. If necessary, interview the Security Directory or equivalent.
	2) Gather evidence that changes made to the group policies are clearly and fully recorded in the Change Control database. Request for a report from the Change Control database, for all group policy changes that occurred in the last three months. Verify the changes with some of the audits carried out in this assignment.
	3) Gather a list from the security and/or system administrator, of GPOs that have restricted permissions applied. Verify that permissions have been restricted appropriately on the specified GPOs. In particular, a subgroup of administrators have been denied the following permissions to the GPOs:
	  ▪ Write
	  ▪ Create All Child Objects
	  ▪ Delete All Child Objects

	Stimulus/Response Testing: 1) Request one of the administrators, who has been restricted from modifying group policies, to logon to the AD domain controller. 2) From 'Active Directory Users and Computers', locate one of the restricted GPOs. 3) In the 'Group Policies Properties' window, highlight a restricted GPO and confirm that the 'Edit' button is dimmed for the particular GPO. 4) With the restricted GPO still highlighted, click the 'Properties' button. 5) In the 'xx Policy Properties' window, select the 'Security' tab. The following error message should display. 6) Attach screenshots and document findings in the audit report. 7) By default, all 'Domain Admins' and 'Enterprise Admins' have the permissions to modify group policies. 8) Attach screenshot and document findings in the audit report.
Objective/ Subjective	Objective

Check #11 – Screen Saver on Domain Controllers

Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm (item 9)
Control objective	Disclosure of proprietary information must be minimized. Screen saver must be password protected, and activated after 3 minutes of inactivity on the Domain Controllers.
Risk	Unauthorized access to proprietary network and directory services details on Domain Controllers, which do not have screen saver turned on, when left unattended.
Likelihood	Medium
Consequence	Potential loss of system availability and integrity, and unauthorised access to confidential corporate data. Also potential loss of credibility.
Compliance/ Expected Results	• Screen saver is enabled and password protected on Domain Controllers. • Screen saver is activated after 3 minutes of inactivity on Domain Controllers.

Testing	1. Request the system administrator to provide screenshots of the screen saver settings for the default Domain Controller policy. The required details are under the 'User Configuration' node, in the Administrative Templates | Control Panel | Display folder.
	
	2. Verify that the following policies are enabled.
	  • Activate screen saver,
	  • Screen saver executable name set to a valid screensaver,
	  • Password protect the screen saver,
	  • Screen saver timeout enabled and set to a period of no more than 180 seconds (3 minutes).
	
	3. Document the findings in the audit report.

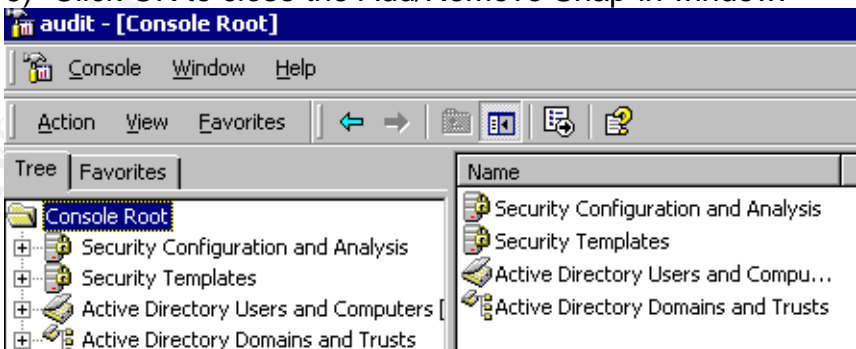| Objective/ Subjective	Objective

Check #12 – Organizational Units

Reference	• Magalhaes, Ricky M. Securing Windows 2000 Active Directory (Part 1). 2 December 2002. http://www.windowsecurity.com/articles/Securing_Windows _2000_Active_Directory_Part_1.html
Control objective	OUs must have the right permissions assigned. Unknown OU objects that were not created by the administrators must be identified and removed. This is also a means of detecting for intruders.
Risk	Organisational units (OUs) not protected and not regularly monitored.
Likelihood	High
Consequence	Incorrectly configured OUs will result in inappropriate inheritance of policies by the OUs, user and computer objects within the OUs. Without regular monitoring, intrusion could happen without being detected and dealt with in a timely manner.
Compliance/ Expected Results	• All OUs are clearly labeled. • No OU object appears without an icon, which the administrators did not create. • OUs have appropriate permissions assigned.
Testing	1) Assume you have completed Check #6. 2) Open the 'audit.msc' MMC created in Check #6. 3) Highlight 'Active Directory Users and Computers' and expand the Domain tree. 4) From the Active Directory Users and Computers MMC console, click View and ensure Advanced Features is checked. The system OUs will then be displayed.

	5) Browse through the AD for OUs that are not labeled or appear without an icon.
	6) To check the security permissions assigned to an OU, right-click on the OU, select Properties, select the Security tab; click the Advanced button to view the full list of permissions.
	7) Ensure appropriate permissions are assigned to the OU.
	8) Document the findings in the report.
Objective/ Subjective	Objective

Check #13 – Domain Trusts

Reference	• Magalhaes, Ricky M. Securing Windows 2000 Active Directory (Part 2). 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows _2000_Active_Directory_Part_2.html Internal resource: system and security administrators
Control objective	Potential security breaches and corruptions caused by remote administrators must be minimized. The need to have two-way transitive trust must be carefully reviewed.
Risk	Inappropriate Domain Trusts
Likelihood	High
Consequence	Potential problems caused by remote administrators, made possible by two-way transitive trust between the forest root and the parent domain and the child domain.
Compliance/ Expected Results	• Use of non-transitive "one way" trusts in cases where a two-way transitive trust is not necessary or where a domain is vulnerable to misuse by remote administrators in other domains.
Testing	1) Interview system and security administrators to determine the organization's domain trust requirements. 2) Verify that domain trusts relationships are clearly documented. 3) Open the 'audit.msc' MMC created in Check #6. 4) From the Console menu, select 'Add/Remove Snap-in'. 5) From the list of available Standalone Snap-ins, select 'Active Directory Domains and Trusts' and click Add. 6) Click OK to close the Add/Remove Snap-in window. 7) From the Console menu, select 'Save' to re-save the 'audit.msc' console. 8) Highlight 'Active Directory Domains and Trusts' and expand the domain tree. 9) Right-click on the domain to be audited, and select Properties.

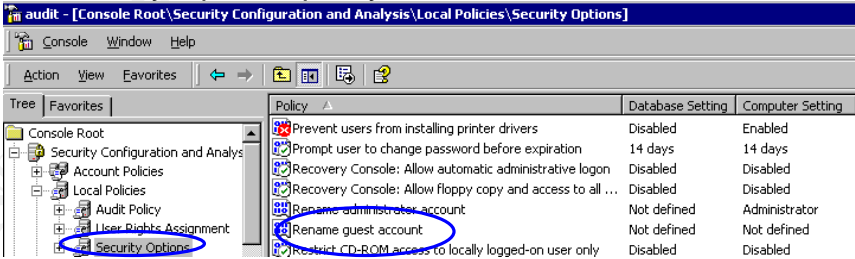| | 10) Select the Trusts tab to display all the domain trusts currently configured. |
	11) Verify the system settings against the requirements.
	12) Document findings in the report.
Objective/ Subjective	Objective

Check #14 – Documentation of GPOs

Reference	• netiQ. Securely Managing Your Group Policies. White Paper. http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf
Control objective	The integrity and availability of the AD and GPOs must be maintained. The design of the AD and GPOs settings must be fully documented. For ease of administration of GPOs at the GPO level within an AD, a product like NetIQ Group Policy Administrator is highly recommended.
Risk	GPOs not documented.
Likelihood	High
Consequence	In the situation of an AD catastrophe, a full recovery of group policies, which consist of over 680 configurable settings per GPO, may not be possible. It would also be difficult to troubleshoot policy related problems if GPOs are not fully documented.
Compliance/ Expected Results	Up to date internal documents are available with the following details: • who are responsible for the GPOs in each domain, • full list of GPOs and where are they applied, • comprehensive documentation of each GPO, including all settings that are different from the defaults, at the minimal.
Testing	Gather evidence of up to date documents containing: 1) responsibilities for the GPOs in each domain, 2) full list of GPO links and where are they applied, 3) comprehensive documentation of each GPO, including all settings that are different from the defaults, at the minimal. 4) Open the 'audit.msc' MMC created in Check #1. 5) Highlight 'Active Directory Users and Computers' and expand the Domain tree. 6) Highlight the desired domain node. 7) Right-click on an OU and select Properties. 8) Select the Group Policy tab. 9) Click Add. 10) In the 'Add a Group Policy Object Link' window, select the 'All' tab. **Add a Group Policy Object Link** Domains/OUs | Sites | All 11) Select a few critical GPO links and verify the system
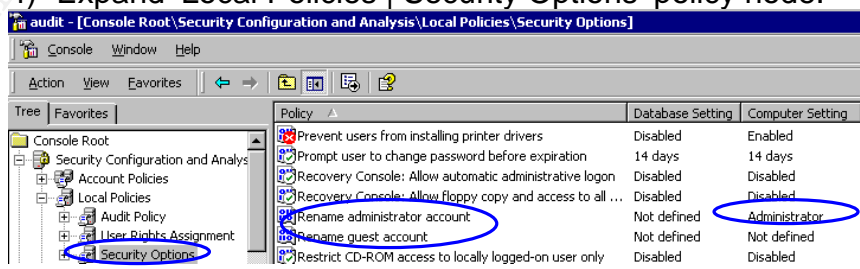
	settings against the documentation.
	12)Document the findings in the report.
Objective/ Subjective	Objective

Check #15 – Guest Account

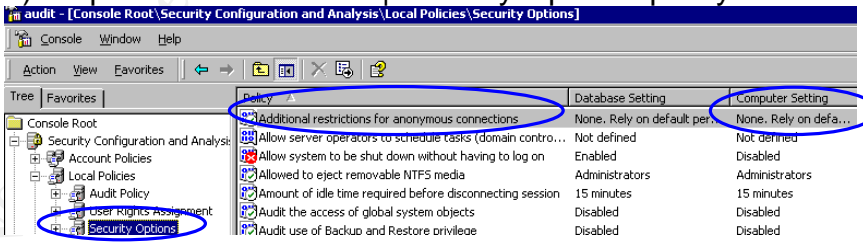|	
Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm
Control objective	Appropriate authentication and authorized access to the system must be maintained.
Risk	The Guest account is not disabled.
Likelihood	Low
Consequence	Misuse of services that have inadvertently left open using the Guest account, which allows anonymous access to computer.
Compliance/ Expected Results	• The Guest account is disabled. • For further security, the Guest account is also renamed.
Testing	1) Assume you have completed Check #6. 2) Open the 'audit.msc' MMC created in Check #6. 3) Expand the 'Security Configuration and Analysis' scope item. 4) Expand the domain to be audited. 5) Select the default 'Users' container. 6) Make sure there is a red X against the Guest account. 7) With 'audit.msc' still open, expand 'Local Policies | Security Options' policy node. 8) Verify that the Computer Setting for the 'Rename guest account' policy is not set to 'Not defined'. 9) Attach screenshots and document findings in the report.
Objective/ Subjective	Objective

Check #16 – Administrator Account

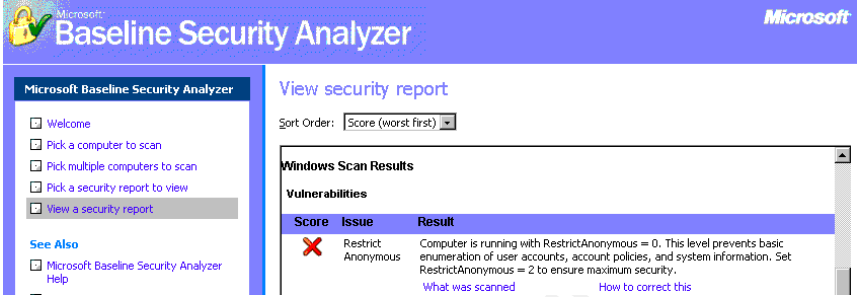| Reference	• Magalhaes, Ricky M. Securing Windows 2000 Active Directory (Part 1). 2 December 2002. http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_1.html
Control objective	To make it more difficult for hackers to find the 'Administrator' username, by renaming it to something that sounds like an ordinary username.
Risk	The default Administrator account is not renamed.
Likelihood	High
Consequence	Since the 'Administrator' username cannot be locked out, hackers can try as many times as they like to hack and crack its password. After successfully finding the 'Administrator' username and password, hackers can then use it to hack other local accounts. With the elevated privileges of the default 'Administrator' account, the security of the AD infrastructure can be compromised, affecting its integrity and availability.
Compliance/ Expected Results	• The default Administrator account in each domain is renamed to an account name that complies with the standard naming convention for a general user account; hence it is not easy to spot the account. • A decoy 'Administrator' account has been created that has NO privileges to anything and a complex 10-digit password. Furthermore, the decoy account has a login script that writes the client machine's host name and IP address to a file whenever someone is able to log in using it, and then deal with the user or hacker.
Testing	1) Ensure you have completed Check #6. 2) Open the 'audit.msc' MMC created in Check #6. 3) Expand the 'Security Configuration and Analysis' scope item. 4) Expand 'Local Policies | Security Options' policy node. 5) Verify that the Computer Setting for the 'Rename administrator account' policy is not set to the default 'Administrator'. That is, the Domain Administrator

	account has been renamed.
	6) From 'Active Directory users and Computer', do a 'Find' for the renamed Domain Administrator account.
	7) Verify that the text in the 'Description' field for the account has also been changed.
	8) Next, do a 'Find' for 'Administrator', a decoy user account and verify that it has no special permissions or user rights.
	9) Attach screenshots and document findings in the report.
Objective/ Subjective	Objective

Check #17 – Anonymous Users

Reference	• SANS. Basic Security Issues of Active Directory. 11 June 2001. http://www.sans.org/rr/win2000/active_dir.php • Microsoft Baseline Security Analyzer http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link)
Control objective	Anonymous users must be disallowed, to insure the confidentiality and availability of the AD are maintained.
Risk	Anonymous user not disabled.
Likelihood	High
Consequence	Potential unauthorized access because anonymous users can enumerate the names of domain accounts and network shares. Malicious users could take advantage of this vulnerability to obtain critical information pertaining to an internal network, and launch an attack or gain unauthorized access.
Compliance/ Expected Results	• The 'Additional restrictions for anonymous connections' security policy is set to 'No access without explicit anonymous permissions'.
Testing	1) Assume you have completed Check #6. 2) Open the 'audit.msc' MMC created in Check 6. 3) Expand the 'Security Configuration and Analysis' scope item. 4) Expand 'Local Policies | Security Options' policy node. 5) Verify that the Computer Setting for the 'Additional restrictions for anonymous connections' security policy is set to 'No access without explicit anonymous permissions'. 6) Can also use the Microsoft Baseline Security Analyzer to test whether the server is protected from anonymous logon. 7) Run Microsoft Baseline Security Analyzer to scan the domain controllers to be audited, by specifying a range of IP address. 8) From the security report generated from running

	Baseline Security Analyzer, scroll down to the Windows Scan Results section.
	9) Under Vulnerabilities, make sure there is a green tick and not a red X against the Restrict Anonymous issue.
	10) Attach screenshots and document findings in the report.
Objective/ Subjective	Objective

Check #18 – NTFS

Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm • Microsoft Baseline Security Analyzer (MBSA) http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link)
Control objective	The reliability, security and availability of the AD domain must be maintained. NTFS file system must be used. NTFS partitions offer access controls and protections that aren't available with the FAT, FAT32, or FAT32x file systems.
Risk	Drives are not formatted NTFS
Likelihood	Low
Consequence	Domain controllers and large drives require NTFS. Lack of reliability and security with the FAT and FAT32 file systems.
Compliance/ Expected Results	• All hard drives are using the NTFS file system.
Testing	1) Download and install MBSA. 2) Run MBSA to scan the AD servers. (acquire necessary admin rights from the system administrator) 3) From the security report locate the 'Windows Scan Results' section. 4) For the 'File System' issue, click 'Result details'.

Baseline Security Analyzer

All hard drives (1) are using the NTFS file system.

Result Details

Score	Drive Letter	File System
✔	C:	NTFS

	5) Confirm that all hard drives are using the NTFS file system.
	6) Document findings in the audit report.
Objective/ Subjective	Objective

Check #19 – Inactive Accounts
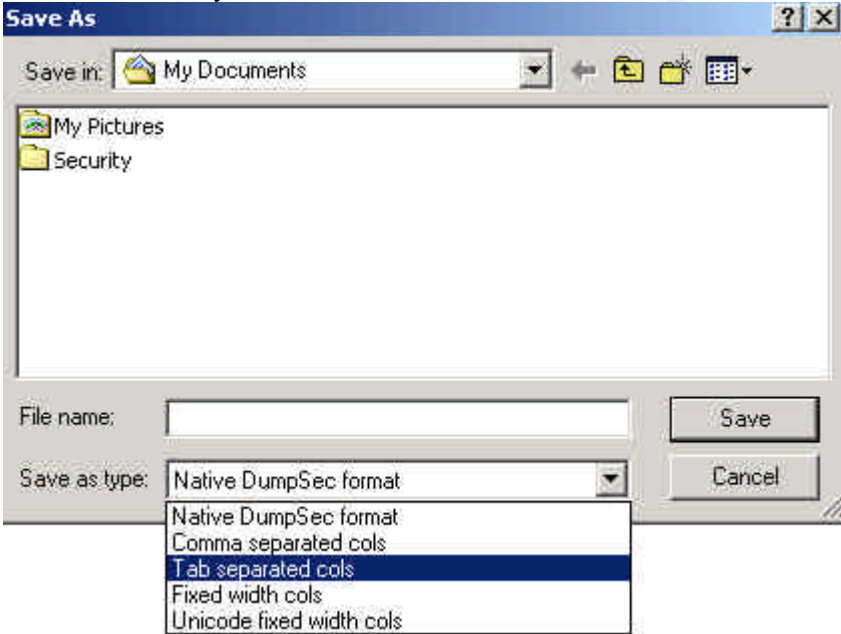
Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm • SomarSoft Utilities. DumpSec http://www.somarsoft.com/ (download link)
Control objective	Confidentiality, integrity and availability of the AD infrastructure must be maintained. Must minimize the exposure to risk of unauthorised access to the system, by malicious users who leverage the redundant accounts and file shares as entries to the local system.
Risk	Inactive and redundant accounts not disabled or deleted. Such accounts are subject to unauthorised usage.
Likelihood	High
Consequence	Potential exposure to unauthorized access to the system, making use of inactive or redundant accounts, and the redundant file shares. In addition, accounts having 'admin' permissions can be used to further exploit any known vulnerabilities within the AD infrastructure.
Compliance/ Expected Results	• Minimal inactive and redundant user accounts, test and shared accounts.
Testing	1) Download the SomarSoft DumpSec utility. 2) Provide the system administrator the utility and instructions for installing the utility. 3) Provide the system administrator the following instructions for generating the required reports from the DumpSec utility. 4) Run DumpSec. (from the administrator's workstation) 5) From the 'Report' menu select 'Select Computer…'. 6) Enter the name of the server to be audited and click OK. 7) From the 'Report' menu select 'Dump Users as table…'.
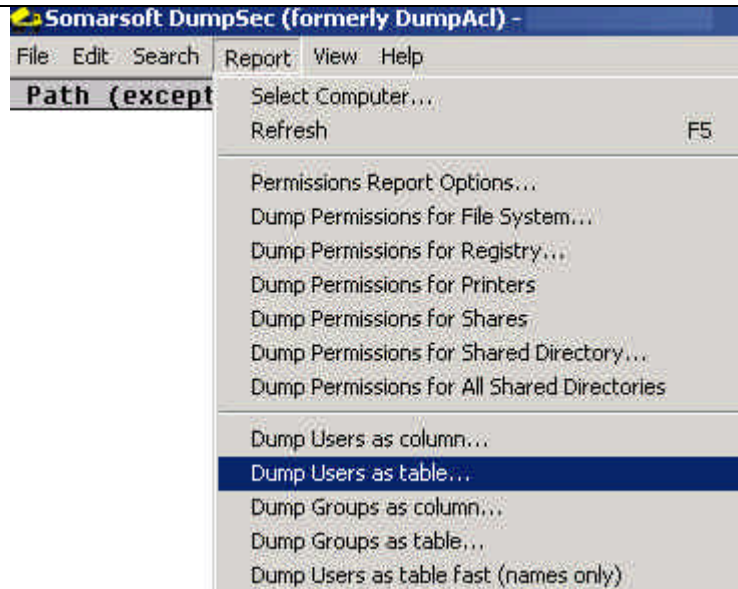
8) From the list of available fields, highlight the required field and click Add. Repeat till all the required fields are added.
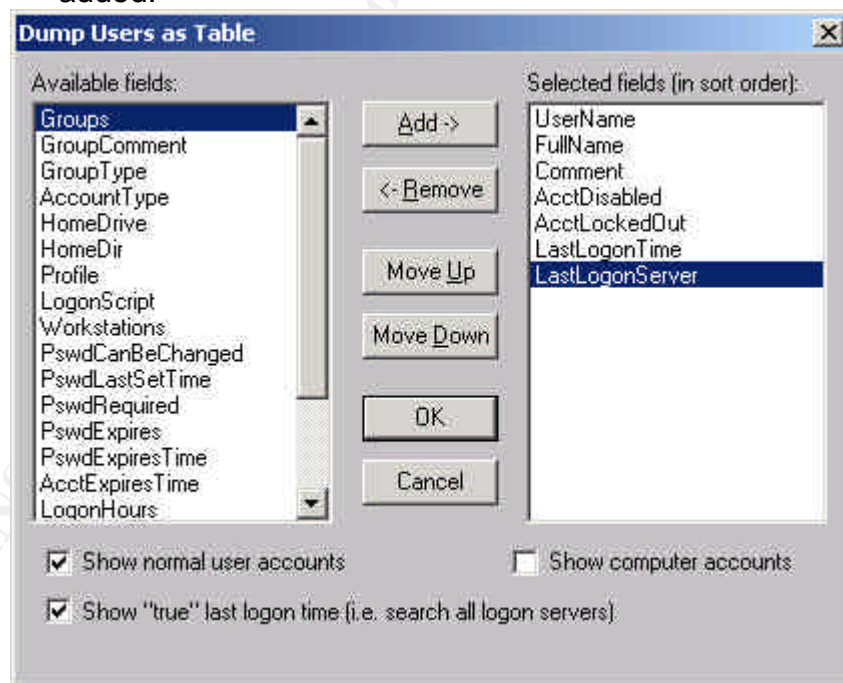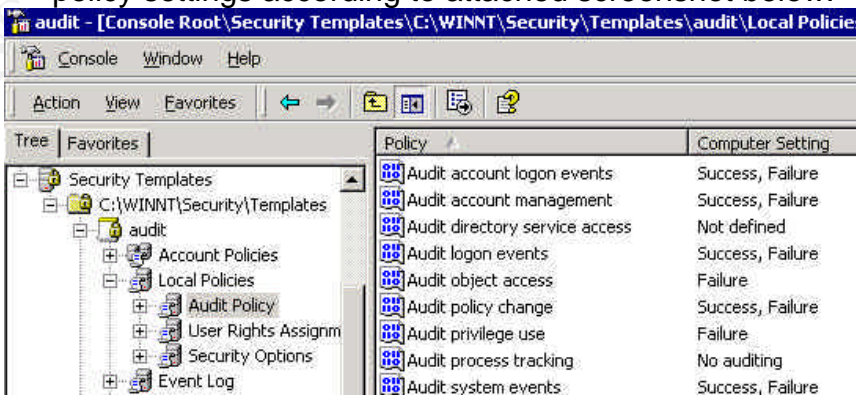
9) Check the box for 'Show "true" logon time (i.e. search logon servers)'.
10) Click OK.
11) On completion, click File | Save Report As…

Somarsoft DumpSec (formerly Du

File Edit Search Report View Help

Save Report As...	Ctrl+S
Load Native File...	
Load Multiple Native Files...	

12) Save the output file to an appropriate file type, this can then be imported into a spreadsheet or database for further analysis.

Save As ? ☒

Save in: 🗀 My Documents ▼ ← 🔁 📑 ▦▾

🖼 My Pictures
🗀 Security

File name: _____ **Save**

Save as type: Native DumpSec format ▼ **Cancel**

Native DumpSec format
Comma separated cols
Tab separated cols
Fixed width cols
Unicode fixed width cols

13) Analyze the 'TrueLastLogonTime' column in order to identify inactive user accounts.
14) Analyse the output file for redundant user accounts.
15) Document findings in audit report.

| Objective/ Subjective | Objective |

Check #20 – Auditing Policy

Reference	• Internal documentation on group policies for Domains, Domain Controllers. • Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I. Version 1.0 (Chapter 4, *Tables 16, 30*) http://www.microsoft.com/downloads/details.aspx?displayla ng=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link)
Control objective	The confidentiality, integrity and availability of the AD must be maintained. Subsequently, auditing must be enabled on domain controllers, servers and computers. This can be managed efficiently with group policies on the various OUs containing the domain controllers, servers or computers.
Risk	Auditing not enabled and system administrators not analysing log files regularly.
Likelihood	High
Consequence	Unauthorized access and malicious activities could occur on the AD without being logged, making detection of malicious activities impossible.
Compliance/ Expected Results	• Auditing policies are enabled with similar settings to best practice. • Event Log policies are enabled with similar settings to best practice.
Testing	1) Assume you have completed Check #6. 2) From the auditor workstation, open the 'audit' MMC console created in Check #6. 3) Expand the 'Security Templates' node and select the 'audit' template. 4) Expand Local Policies | Audit Policy and modify the policy settings according to attached screenshot below. 5) Expand Event Log | Settings for Event Log and modify the policies according to the attached screenshot below.

	These settings can vary depending on the size of the domain. In this example the AD has not been running for very long and has less than 500 objects.
	6) Highlight the 'audit' template, select Action | Save As to re-save the 'audit' template.
7) Right-click the 'Security Configuration and Analysis' scope item, and select 'Open database…'.
8) In the 'Open database' window, select 'audit.sdb' and click 'Open'.
9) Right-click the 'Security Configuration and Analysis' scope item again, and select 'Import Template…'.
10) In the 'Import Template' window select 'audit.inf', and click 'Open'.
11) Right-click 'Security Configuration and Analysis' and select 'Analyze Computer Now'.
12) On completion of analysis, expand the 'Security Configuration and Analysis' scope item.
13) Expand Local Policies | Audit Policy.
14) In the details pane, investigate policies that are marked with a red X. These are computer settings that deviate from the database settings. A green tick indicates that the computer setting complies with the database setting.
15) Expand Event Log | Settings for Event Logs.
16) Investigate computer settings that deviate from the database settings.
17) From the 'Console' menu select 'Save-As' to re-save the MMC console.
18) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective
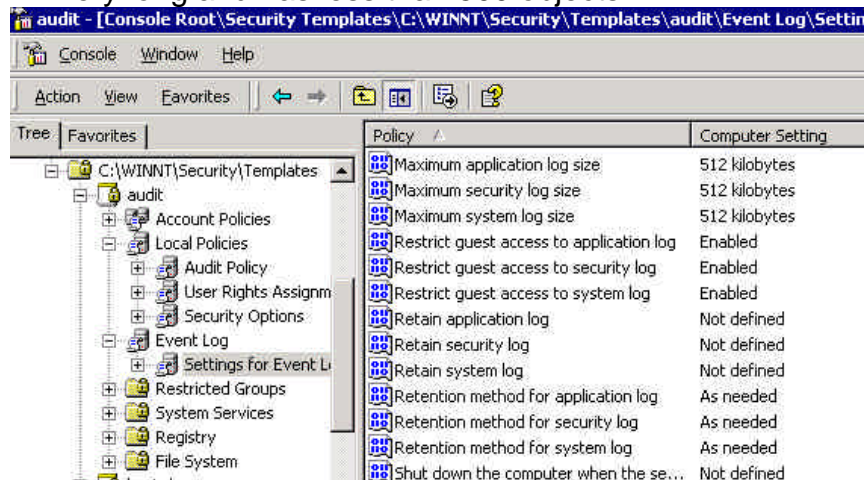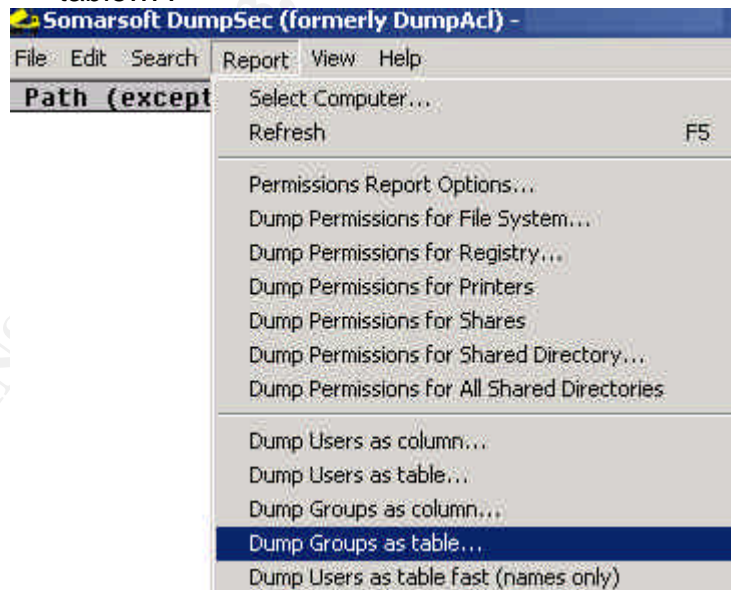
Check #21 – Separating Administrator and User Accounts for Administrative Users

Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm • SomarSoft Utilities. DumpSec http://www.somarsoft.com/ (download link)
Control objective	Confidentiality, integrity, availability and credibility of the network must be maintained. Administrators must have one regular user account for running non-administrative programs, and at least one other account for administrative tasks, in order to minimize the exposure of service administrator accounts.
Risk	Administrators use single logon accounts for everything, including non-administrative tasks, for example, running Office applications and reading e-mail.
Likelihood	High
Consequence	If an attack is successful, an intruder could leverage the 'admin' privileges of the administrators, and cause significant damage to the AD infrastructure.

Compliance/
Expected
Results
	• Administrators with privileged access have separate 'admin' accounts at different hierarchies of the AD. For example, a system administrator has three logon accounts, two accounts for two different administrative roles, and the third account for use as a regular user.
	  ▪ First account – for logon to the Root Domain as a Schema/Enterprise Admin,
	  ▪ Second account – for logon to a Child Domain as a Domain Admin,
	  ▪ Third account – for logon to a Child Domain as a regular user.
	• Furthermore, the administrative accounts are not mail enabled and are not used for running Office applications and browsing the Internet.

Testing	1) Request the system administrator to logon to one of the AD domain controllers. 2) Based on the defined roles and responsibilities for the management of the AD, verify that the administrator has multiple logon accounts. This can be achieved by running 'Active Directory Users and Computers' and do a 'Find' for the name of the administrator. Should find multiple accounts for the administrator in a Child Domain. 3) Confirm that the administrator cannot logon to a Root Domain using his or her 'Domain Admin' user account.
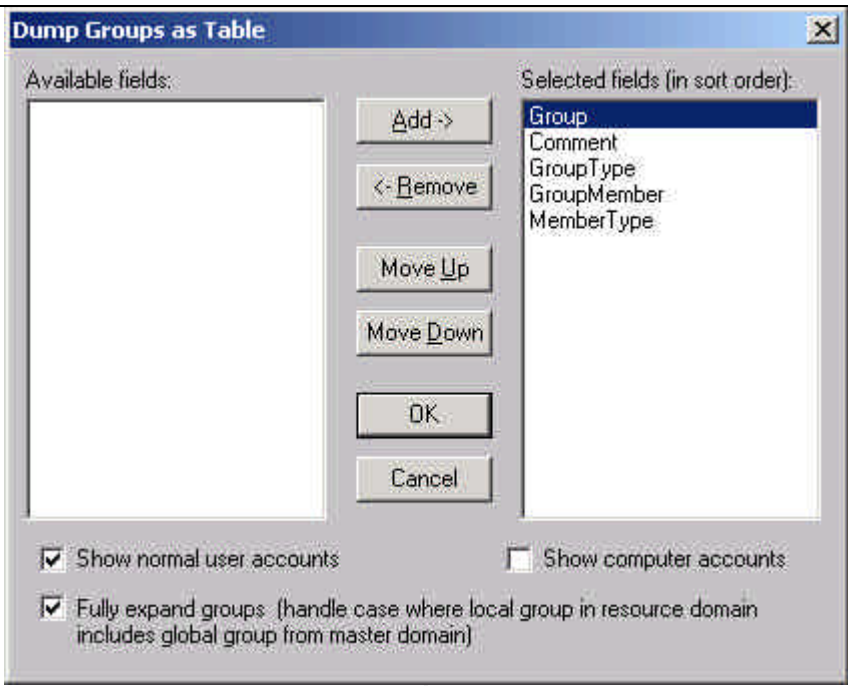
	4) If the administrator is also an Enterprise Admin, request the administrator to logon to the Root Domain using his or her Enterprise Admin user account. 5) Repeat the 'Find' process for the administrator's name in the Root Domain. 6) Document the findings in the audit report. Alternatively, 1) Download the SomarSoft DumpSec utility. 2) Provide the system administrator the utility and instructions for installing the utility. 3) Provide the system administrator the following instructions for generating the required reports from the DumpSec utility. 4) Run DumpSec. (from the administrator's workstation) 5) From the 'Report' menu select 'Select Computer…'. 6) Enter the name of the server to be audited and click OK. 7) From the 'Report' menu select 'Dump Groups as table…'. 8) From the list of available fields, highlight the required field and click Add. Repeat till all the required fields are added, then click OK.

9) On completion, click File | Save Report As…

10) Save the output file to the 'Tab separated cols' file type, which can then be imported into a spreadsheet or database for further analysis.

Save As

Save in: My Documents

My Pictures
Security

File name:

Save as type: Native DumpSec format

Native DumpSec format
Comma separated cols
Tab separated cols
Fixed width cols
Unicode fixed width cols

Save

Cancel

	11) Analyze the following groups at the minimum. • Enterprise Admins – in the Root Domain • Domain Admins • Administrators • Account Operators 12) Document findings in audit report.
Objective/ Subjective	Objective

Check #22 – Securing Domain Master Roles

Reference	• Magalhaes, Ricky M. Securing Windows 2000 Active Directory (Part 2). 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_2.html
Control objective	To maintain the integrity and availability of the AD, the schema master must be protected because only this domain controller can write to the directory schema.
Risk	Domain master roles not secured.
Likelihood	Medium
Consequence	Failure to write to directory schema. Failure to add or remove domains.
Compliance/ Expected Results	• The Enterprise Admin group contains limited number of administrative user accounts, which are used solely for the installation and maintenance of the AD Schema, Domain Naming Master, Domain Trusts, Operations Master, Global Catalog Server, DNS, and RID Master. • The user accounts in the Enterprise Admin group are not used for daily operations tasks, and their passwords are stored away in a security safe. • No occurrence of any disabled domain controller that might hold a schema master, domain-naming master, RID master, or is a Global Catalog Server.
Testing	1) Ascertain that the Enterprise Admin group contains limited number of administrative user accounts. (run the Somarsoft DumpSec utility to extract and then analyze the group memberships of Enterprise Admin, as in Check #22, p.65) 2) Ascertain that the administrators have separate user accounts for use as a general user, Domain Admin, and Enterprise Admin. (Check #22, p.65) 3) Request the administrator to logon to the Root Domain of each site, using an appropriate use account, and repeat Check#1, p.16. From the list of domain controllers found, ascertain that there is no disabled domain controller. If there is, ascertain that the disabled domain controller does not hold a domain-naming master, operations master, or RID master role, or is a Global Catalog Server. 4) Working with the system administrator, find out which Domain Controller holds the operations master role, by running 'Active Directory Domains and Trusts'.
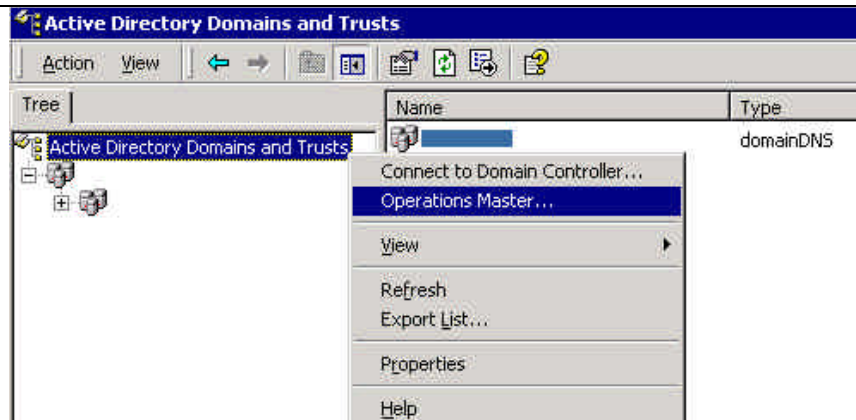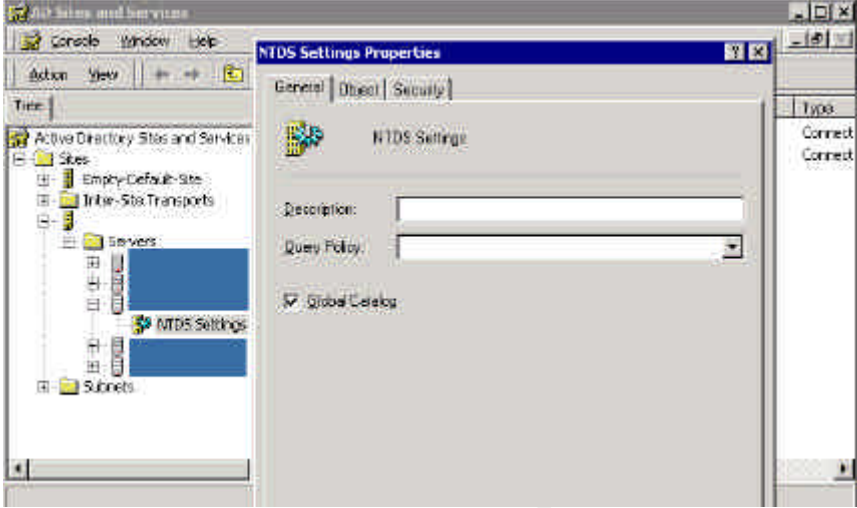
5) Right-click the 'Active Directory Domains and Trusts'
   node, and select 'Operations Master …'. (or select
   'Operations Master …' from the 'Action' menu. The
   'Change Operations Master' screen will be displayed.
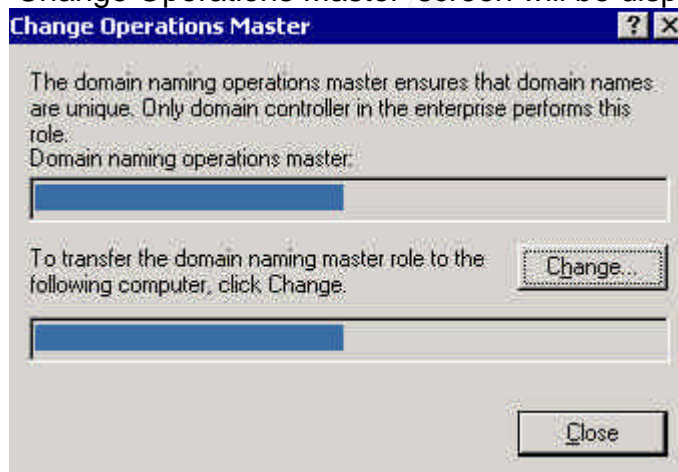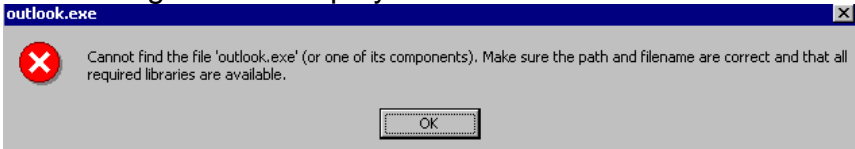
6) Click the 'Close' button and exit 'Active Directory
   Domains and Trusts'.
7) To check whether the particular Domain Controller is a
   'Global Catalog' server, run 'Active Directory Sites and
   Services'.
8) Expand the Sites folder | Empty-Default-Site node |
   Servers folder.
9) From the Servers folder, expand a particular Server
   node.
10) Right-click on 'NTDS Settings' and select 'Properties'.
11) From the 'NTDS Settings Properties' screen, look for the
    'Global Catalog' checkbox, to ascertain whether a
    Server is a 'Global Catalog' Server.

	12)Click 'Cancel' and exit 'AD Sites and Services'.
	13)Logoff from the Domain Controller.
	14)System Administrators should run the 'Netdiag' and 'Dcdiag' Active Directory Support Tools on a regular basis, to analyze the state of the Domain Controllers and troubleshoot any report problems on a timely basis.
	15)Document findings in the audit report.
Objective/ Subjective	Objective

Check #23 – Reading of Email

Reference	• Windows 2000 Server Baseline Security Checklist http://w2kinfo.nacs.uci.edu/Member_server_baseline_sec.htm
Control objective	The loss of system availability and business productivity must be minimized. Apart from the email client, office productivity applications and utilities that are not strictly required by the server must not be installed.
Risk	Reading of email on the AD servers (or any server)
Likelihood	Medium
Consequence	Potential of a denial of service attack from email virus, or executable attachment containing malicious code
Compliance/ Expected Results	• No email application is installed on the AD servers. For example, Microsoft Outlook or Outlook Express. • Have a policy in place against the reading of email from Servers.
Testing	1) Request a system administrator to logon to the AD server to be audited. 2) From the AD server, click Start | Settings | Control Panel. 3) Double-click Add/Remove Programs. 4) From the list of programs installed, verify that an email client, office productivity applications and unnecessary utilities are not installed on the AD server. 5) Additionally, from the 'Start' menu, verify the applications that can be run from the Servers. *Stimulus/Response Testing:* 1) With the system administrator's logon to the AD server, verify that you cannot run the email client. 2) For example, if you are testing for Microsoft Outlook, go to Start | Run, enter 'outlook.exe' and press Enter. 3) If Outlook is not installed on the machine an error message will be displayed. **outlook.exe** ❌ Cannot find the file 'outlook.exe' (or one of its components). Make sure the path and filename are correct and that all required libraries are available. OK 4) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective

Internal Processes, Policies and Procedures

Check #24 – Antivirus Software

Reference	• Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm • Internal policy for antivirus software on desktops and servers.
Control objective	System corruption and disruption to operations/loss of productivity, as a result of a virus attack, must be minimized
Risk	Antivirus software not installed and virus signatures not up-to-date.
Likelihood	Medium
Consequence	The lack of antivirus software or outdated virus signatures can compromise the security of the system, against malicious code, virus and Trojan horses.
Compliance/ Expected Results	• Antivirus software is installed on the AD server. • Antivirus software is started on the AD server. • Antivirus signature file is up to date.
Testing	1) Request a system administrator to logon to the AD server to be audited. 2) From the AD server, click Start | Settings | Control Panel. 3) Double-click Add/Remove Programs. From the list of programs installed, verify that an email client, office productivity applications and unnecessary utilities are not installed on the AD server. 4) Document findings in the audit report.
Objective/ Subjective	Objective

Check #25 – Active Directory Backup and Restore

Reference	• netiQ. Securely Managing Your Group Policies. White Paper, 11 March 2002. http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf • Internal system backup procedure and schedule • SANS. Basic Security Issues of Active Directory. 11 June 2001. http://www.sans.org/rr/win2000/active_dir.php • Securing Windows 2000 Active Directory (Part 3) – Backup and Restoration. 6 January 2003. http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_3__Backup_and_Restoration.html
Control objective	Availability and integrity of the AD infrastructure must be maintained. There must be regular full backups of all the AD domain controllers including the system state, and restore process for the AD must be tested.
Risk	The AD database and GPOs not backed up and restore not tested or no restore process is available.
Likelihood	High
Consequence	High impact on the availability of the AD and GPOs. In worst cases, it could take days or weeks to rebuild the entire AD. It would also be extremely time-consuming to recreate GPOs, especially if not documented. Without appropriate GPOs the integrity of the AD infrastructure could be compromised.
Compliance/ Expected Results	• Backup schedule for all the domain controllers must exist, where FULL backup on the AD is performed regularly. • Backup logs must exist for all the domain controllers, and that they show evidence of full backup including the system state, and do not contain errors. • Restore process for the domain controllers and the related logs must exist.
Testing	1) Request from the system administrators the backup schedule for all domain controllers. 2) Obtain backup logs from the system administrators for proof of regular and successful full backups of all the domain controllers, including the system state. Verify the handling of backup errors, if any. 3) Verify that the restore process is in place and it's prudent for a full recovery of the AD.
Objective/	Objective

Subjective	

Note: A program similar to the NetIQ Group Policy Administrator can be used to efficiently maintain the GPOs, including backup and restore of selective GPO.

Check #26 – Physical Security

Reference	• Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I. Version 1.0 http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link)
Control objective	Warranty from vendor must not be void; resulting in financial loss. Confidentiality of intellectual information must be maintained. System integrity and availability must be maintained.
Risk	The AD servers are not physically secured.
Likelihood	Medium
Consequence	Apart from potential physical damage to the servers, there is also exposure to unauthorised access to proprietary information.
Compliance/ Expected Results	• A current Computer room access policy is in place, which ensures the computer room access is limited to operations staff, and the user access matrix is kept up to date. • Access to the computer room is restricted by either a key/lock or other access control mechanisms. • UPSs are used to prevent loss of power to the AD servers. • The computer room is monitored by security cameras, which are monitored by security managers. The hours of monitoring will depend on the type of business. • Visitors are required to record their access to the computer room in a log. • Visitors are not to be left alone in the computer room, without appropriate authorization. • The computer room is equipped with at least one fire extinguisher. Furthermore, the fire extinguisher is of an appropriate type, for example, carbon dioxide. • Backup tapes are stored in locked fireproof safe as well as offsite.
Testing	1) Gather evidence of a current Computer room access policy, which ensures the computer room access is limited to operations staff, and the user access matrix is kept up to date. 2) Review the physical access mechanisms. 3) Confirm the existence of security cameras and fire extinguisher (of an appropriate type) in the computer room.

	4) Confirm the security cameras are active, and images being actively monitored by the security managers.
	5) Gather evidence of a current record of the Visitors Log, which should contain details such as Date/time of visit, full name, company, purpose of visit, check in time, check out time, full name of the internal staff who is responsible for the visitor's access to the computer room.
	6) Gather evidence of the use of fireproof safe for backup tapes that are kept in house, and review if there is offsite storage arrangement for the backup tapes.
	Stimulus/Response Testing:
	1) Request the system administrator to accompany the auditor to the computer room(s).
	2) Confirm that the auditor cannot access the computer room with his or her temporary access card/key.
	3) Confirm the existence of the visitors log and that the auditor is required to record his or her access in the Visitors Log.
	4) Document findings in the audit report.
Objective/ Subjective	Subjective

Check #27 – Change Control Procedure

Reference	• Internal Change Control Management Process
Control objective	Hardware, software and group policy changes to the AD and Domain Controllers must be appropriately managed and monitored. Stability and availability of the AD and user environment must be maintained.
Risk	A current and adequate Change Control Management procedure does not exist. Change Control Management procedures not followed.
Likelihood	Medium
Consequence	Unplanned system downtime caused by incorrect or inadvertent changes made to either the AD or Domain Controllers. Uninformed changes to the user environment.
Compliance/ Expected Results	• A current and adequate Change Control Management procedure is in place. • The Change Control Management procedure is followed for all maintenance of the AD and Domain Controllers.
Testing	1) Gather evidence of Change Control completed for all AD related changes implemented over the last three months.
Objective/ Subjective	Objective

Assignment 3 – Conduct the Audit

The ten items shown below are the areas that I believe reflect the most significant security concerns and are most critical to the success of this audit.

Audit #1 – Domain Controllers

Reference	• Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 2)". 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_2.html
Control objective	Since Domain controllers contain sensitive data used for authentication, its availability must be maintained at all time. Domain controllers must be physically secured. Access to the Domain controllers must be restricted to a small group of authorized and skilled personnel.
Risk	Inadequate protection for the Domain Controllers.
Likelihood	High
Consequence	Failure of a domain controller, especially if fault tolerance does not exist, will stop domain authentication from working.
Compliance/ Expected Results	• For redundancy, more than one domain controllers exist in the Root Domain and Child Domains. • Domain controllers are physically secured in computer rooms where access is tightly controlled. • A current Computer Room Access Policy is in place. • Remote Access to the Domain Controllers is restricted.
Testing	1) From the auditor workstation run 'Active Directory Users and Computers'. 2) Right-click on the domain to be audited, and select 'Find…' 3) In the 'Find' selection box, select 'Computers'. 4) In the 'In' selection box, select 'Entire Directory' (or select the Root Domain followed by individual Child Domain). 5) Click 'Find Now' to continue.
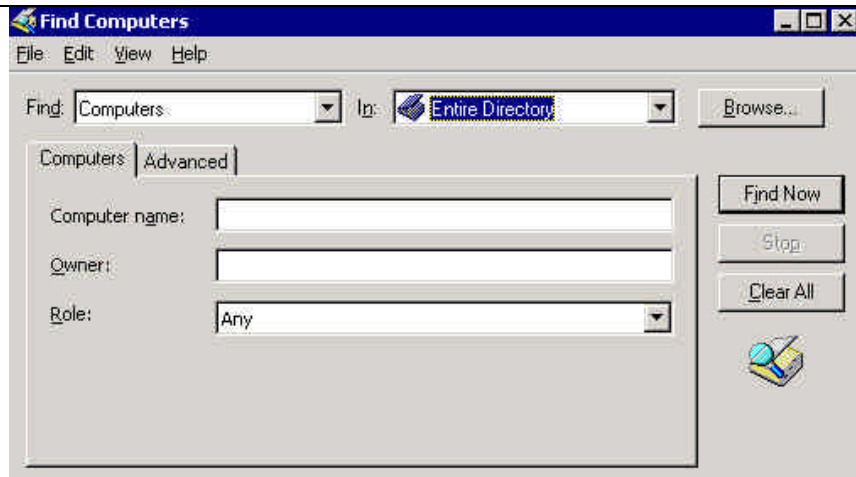
6) In the display pane of the Find Computers window, click the Machine Role column header, to sort the computers by type.
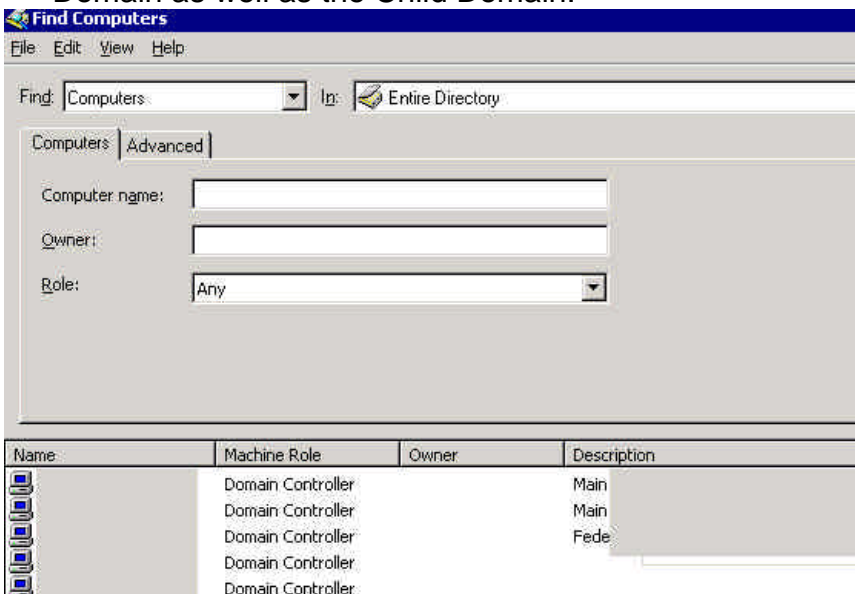
7) Gather evidence that multiple computers are listed as having the Domain Controller machine role.
8) Request the administrator to provide the Physical Access User Access Matrix, and perform test on a random sample to confirm who in the IT department can/cannot access the computer rooms.
9) Run 'Administrative Tools | Terminal Services Configuration' from the Domain Controllers.
10) Select the 'Connections' folder.
11) In the details pane on the right, right-click on the 'RDP-Tcp' connection and select 'Properties'.
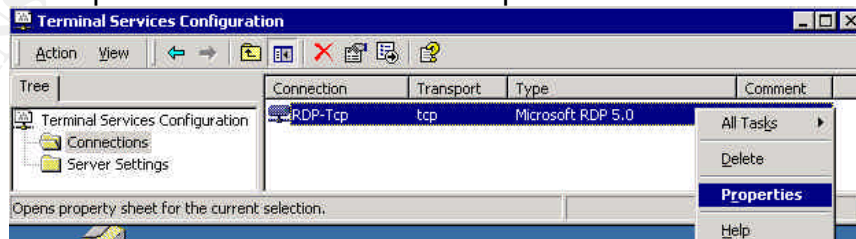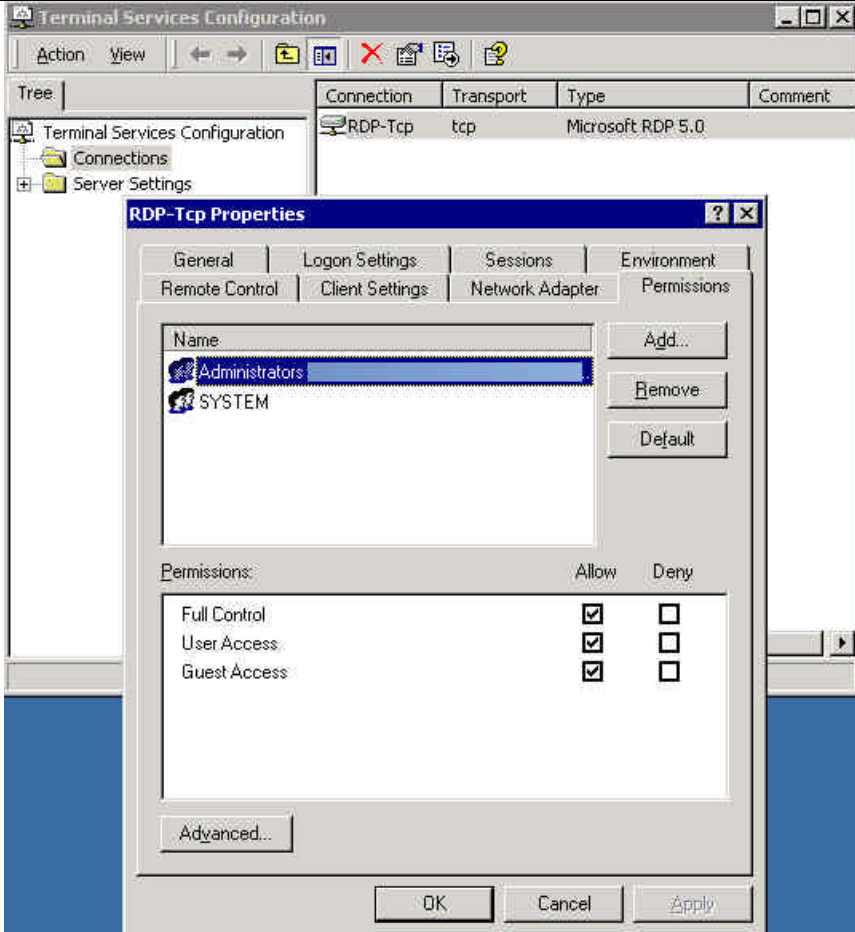
12) Click the 'Permissions' tab and analyze who have remote access to the Domain Controllers from running Terminal Services.
13) Document the findings in the audit report.
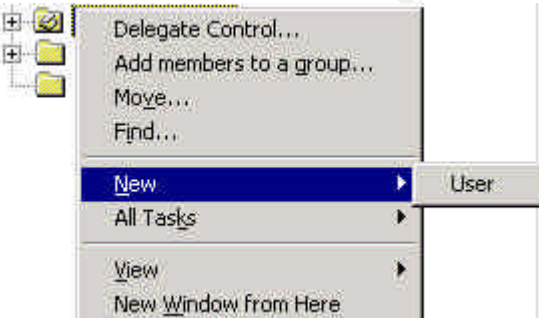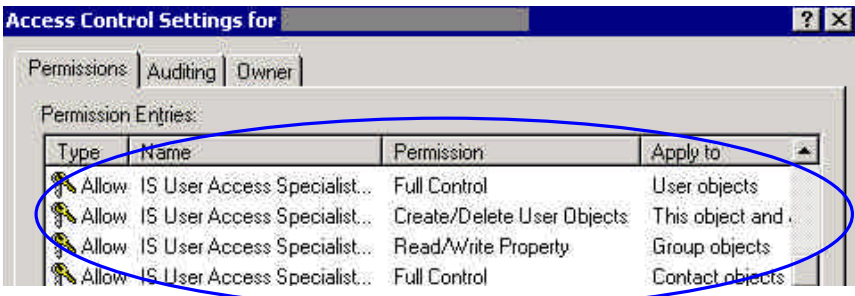
Objective/	Objective
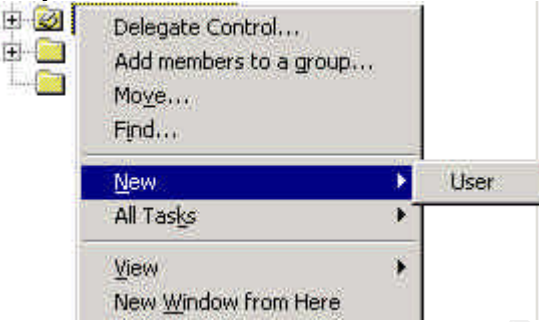
Subjective	
Test Results	• There are multiple Domain Controllers found in the Root Domain as well as the Child Domain.

• The Physical Access User Access Matrix is well documented.
• From the random sample of physical access cards that I have tested, a number of temporary access cards have been granted access to the computer rooms, where the AD Domain Controllers as well as most of the business critical application Servers are stored. It has been noted that the 'card access or SSM' system is controlled and maintained by a separate Security and Surveillance department. However, the information concerning what level of access to be granted to a particular IT department owned access card comes from the IT department.
• The remote access test passed whereby only appropriate users are allowed this access to the AD Domain Controllers, from running Terminal Services.

| Auditor Notes | Compliance test failed the physical access test. All other tests passed. |

Audit #2 – Delegating Administrative Control of the AD Objects
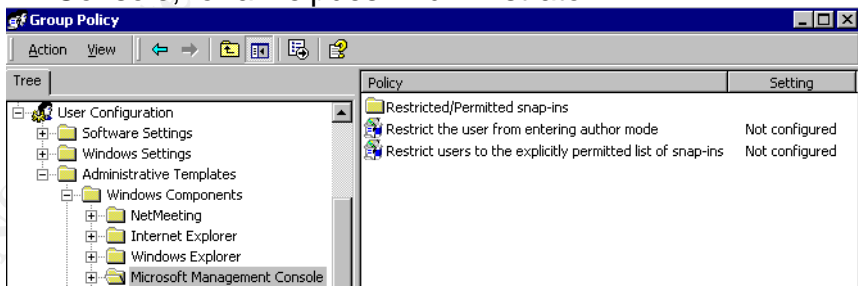
Reference	• Internal documentation of various roles and responsibilities for the AD
Control objective	Integrity of the AD and its availability must be maintained. Administrative roles and responsibilities must be clearly defined. The ability of individuals to perform certain AD administrative functions must be appropriately controlled. Unauthorised access to information in the AD must be minimized.
Risk	Lack of clearly defined roles and responsibilities for the administration of the AD, and inappropriate delegation of administrative control for the AD objects.
Likelihood	High
Consequence	Poor management and unauthorised access to the AD infrastructure, which could have high impact on the availability of the AD. The end result would be a lack of accountability for changes occurred and ownership for problems resolution, resulting in poor service delivery to the users.
Compliance/ Expected Results	1) Roles and responsibilities for the administration of the AD are clearly defined and documented. 2) The roles of Schema Admin, Enterprise Admin, Domain Admin, Backup Operators and Server Operators, are assigned to system administrators, based on their roles and responsibilities for the AD. Hence different levels of administrators have different delegated authorities over different portions of the AD. For example, a Helpdesk Administrator who is tasked with the 'Password Reset' and 'Unlock User Account' administrative role will be granted with appropriate permissions on only the user objects. The Helpdesk Administrator will not have the authority to manage computer objects, which is a task of the technicians or system administrators.
Testing	1) From the auditor workstation, run 'Active Directory Users and Computers'. 2) Select the domain node to be audited. 3) Right-click on the domain OU and select Properties. 4) From the *domain* Properties window select 'Security'. 5) Click the 'Advanced…' button to view additional permissions. 6) From the Access Control Settings for <*domain*> window, select the 'Permissions' tab (by default).

	7) From the list of permission entries, locate entries that are related to 'User Access Specialist', who are responsible for the maintenance of user accounts and groups. 8) Make sure the 'User Access Specialist' administrative role is only granted specific permissions for the management of user and user group objects. 9) Click 'Cancel' a couple of times to close the open windows. *Stimulus/Response Testing:* 1) Request one of the User Access Specialists to logon to the domain to be audited. 2) Run Active Directory Users and Computers. 3) Expand the domain node. 4) Right-click on an OU. 5) Select New. 6) Confirm that only the 'User' object is available. 7) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective
Test Results	• The test shows that the 'IS User Access Specialists' administrative role is granted only specific permissions to the User, Group and Contact objects, which are required for maintaining user accounts and groups. The test results are as shown below.

	• It is also tested that a User Access Specialist can only create a new user object, but not computer or other objects in the AD.
Auditor Notes	Compliance test passed.

Audit #3 – MMC Consoles

Reference	• Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 2)". 20 December 2002. http://www.windowsecurity.com/articles/Securing_Windows _2000_Active_Directory_Part_2.html • Internal documentation of administrative roles and responsibilities for the AD.
Control objective	The integrity and availability of the AD must be maintained. The risk of an intruder gaining full control of the admin tools must be minimized. Access to MMC snap-ins must be restricted based on the roles and responsibilities for the AD.
Risk	Access to MMC consoles not restricted, and not inline with the AD administrative roles and responsibilities.
Likelihood	Medium
Consequence	If delegation of administration is lacking or incorrectly configured, an intruder with full control of the admin tools could exploit the admin privileges to gain unauthorized access to information on the AD.
Compliance/ Expected Results	• Permissions to run specific administrative tools are mapped to administrative authorities that have been delegated to a user for an administrative task. • For further security, users can be prevented from running MMC console in author mode.
Testing	1) Request the system administrator to provide screenshots of GPO settings for Microsoft Management Console, for a Helpdesk Administrator. 2) For the Restricted/Permitted snap-ins policies, verify that admin snap-ins, especially 'Active Directory Domains and Trusts', 'Active Directory Sites and Services', 'Security Configuration and Analysis', and 'Security Templates' are restricted from the Helpdesk Administrator. Depending on the environment, some other snap-ins could be restricted too.

3) Depending on the environment, the 'Restrict the user from entering author mode' policy could be enabled to provide further security.

Stimulus/Response Testing:
1) From the Helpdesk Administrator's workstation, click Start | Run.
2) Enter 'mmc' and press Enter.
3) From the Console menu confirm that the Add/Remove Snap-in… option is not available.

4) From the Console menu, select 'Add/Remove Snap-in'.
5) On the 'Add/Remove Snap-in' window, click Add. The 'Add Standalone Snap-in' window will be displayed.

6) Confirm that all the restricted snap-ins do not appear in the list of Available Standalone Snap-ins.
7) Click on Close to close the 'Add Standalone Snap-in' window.
8) Click Cancel to close the 'Add/Remove Snap-in' window.
9) Document findings in audit report.

Objective/ Subjective	Objective
Test Results	• Restrictions on MMC snap-ins have been configured according to the defined roles and responsibilities for the AD. The attached screenshot shows the restricted/permitted snap-ins for the Helpdesk Administrator, where the Active Directory Users and Computers, Domains and Trusts, Sites and Services, and some other snap-ins have been disabled.

	• From a MMC console, when the Helpdesk Administrator tried to add a standalone snap-in, only the permitted snap-ins is available for selection.
Auditor Notes	Compliance test passed.

Audit #4 – AD Access Controls and ACLs

Reference	• Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I". Version 1.0 (*Table 11*) http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link) • Microsoft Baseline Security Analyzer http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link)
Control objective	Unauthorised access to system files and executables, file shares and registry keys must be minimized. The risk of disk-space attacks on AD domain controllers must be minimised. Appropriate ACLs must be applied to registry keys, file system and other data (and log) partitions; in order to maintain the stability and integrity of the AD infrastructure.
Risk	Default AD access permissions and NTFS ACLs are too permissive, granting **Everyone** group **Full Control** permissions on the root of each logical disk volume on the AD, and newly created file shares and registry keys.
Likelihood	High
Consequence	Vulnerability of domain controller to disk-space attacks on each disk volume, including the AD database files volume. Inappropriate access permissions assigned to file shares and registry keys.
Compliance/ Expected Results	• 'Everyone – Full Control' permission is not granted to the root of each logical disk volume. • Files and folders on the domain controllers are appropriately secured, as shown in following table. <table><tr><td>File or Folder</td><td colspan="2">Permissions</td></tr><tr><td>Root of each logical disk volume</td><td>1.</td><td>Allow Read and Execute for Everyone</td></tr><tr><td></td><td>2.</td><td>Allow Full Control for Administrators</td></tr></table> • Default ACL permissions on file shares, file system and registry keys in GPOs modified, with 'Authenticated Users/Appropriate access control' replacing 'Everyone/Full Control' permissions. Also allow 'Full Control' for Administrators.
Testing	<u>AD Access Controls</u> 1) From the auditor workstation, run 'Computer Management'

2) Right-click on 'Computer Management (Local)' and
   select 'Connect to another computer …'.
3) Select a domain controller from the AD and click OK.
4) Expand the 'Storage' node.
5) Click 'Disk Management'.
6) Right-click on the 'root volume', that is, 'C:', and select
   'Properties'.
7) On the 'Local Disk (C:) Properties' screen, select the
   'Security' tab.

	8) Verify that appropriate permissions have been assigned to each user or user group for the root of all logical disk volumes.
	<u>ACLs</u>
	9) Down and install MBSA.
	10) Run MBSA and scan the AD domain controllers.
	11) From MBSA | View Security Report, locate the 'Additional System Information' section.
	12) Select 'Result Details' for the 'Shares' issue.
	13) Verify that appropriate access permissions are assigned to the shares and in particular, 'Everyone' is not granted Full Access to any of the shares.
	14) Document findings in the audit report.
Objective/ Subjective	Objective
Test Results	• Default permissions, Everyone/Full Control, have been assigned to the root of the logical disk volume on all the Domain Controllers.

Local Disk (C:) Properties

General | Tools | Hardware | Sharing | Security | Quota |

Name
Everyone

Add...
Remove

Permissions: Allow   Deny

Full Control   ☑   ☐
Modify   ☑   ☐
Read & Execute   ☑   ☐
List Folder Contents   ☑   ☐
Read   ☑   ☐
Write   ☑   ☐

Advanced...
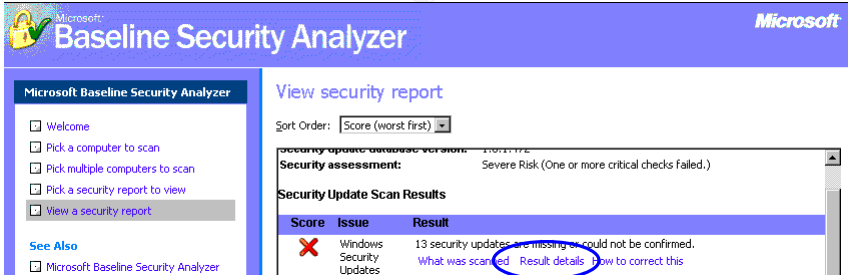
OK   Cancel   Apply

- The results of computer scan from running MBSA confirms that the Admin Share C$ and some other shares are having the default Everyone/Full Control permissions applied.

C$ C:\   Admin Share: Everyone - F

Auditor Notes	Compliance test failed.

Audit #5 – Service Packs and Hotfixes

Reference	• Internal documentation on Service Packs and Hotfixes implementation process and schedule.
Control objective	Exposure to published security threats must be minimized.
Risk	Domain Controllers not kept up-to-date with the latest Service Pack and security Hotfixes.
Likelihood	Medium
Consequence	Exposure to known security threats, through unauthorised access to the system, with elevated privileges at the server level.
Compliance/ Expected Results	• No security updates are reported missing.
Testing	1) Under the 'Security Update Scan Results' section, check the score and result for the 'Windows Security Updates' item. 2) If there are missing security updates, click on the 'Result details' link for further details. 3) Document the findings in the audit report.
Objective/ Subjective	Objective
Test Results	• All the Domain Controllers tested have missing security updates. The attached screenshot shows some of the missing hotfixes.

	Baseline Security Analyzer
	13 security updates are missing or could not be confirmed
	Result Details
	Windows Security Updates
	Security updates confirmed as missing are marked with a red X

Score	Security Update	Description	Reason
✖	MS02-070	Flaw in SMB Signing Could Enable Group Policy to be Modified (329170)	File \\ versio [5.0.2
✖	MS02-071	Flaw in Windows WM_TIMER Message Handling Could Enable Privilege Elevation (328310)	File \\ versio [5.0.2
✖	MS03-001	Unchecked Buffer in Locator Service Could Lead to Code Execution (810833)	File \\ versio [5.0.2
✖	MS03-010	Flaw in RPC Endpoint Mapper Could Allow Denial of Service Attacks (331953)	File \\ [5.0.2
✖	MS03-011	Flaw in Microsoft VM Could Enable System Compromise (816093)	File \\ versio
✖	MS03-013	Buffer Overrun in Windows Kernel Message Handling could Lead to Elevated Privileges (811493)	File \\ [5.0.2
✖	MS03-015	Cumulative Patch for Internet Explorer (813489)	The re Comp

Auditor Notes	Compliance test failed.

Audit #6 – Password Security

Reference	• Internal policy document on logon account and password. • Windows 2000 Security Checklist http://www.labmice.net/articles/securingwin2000.htm (item 8) • @stake LC4 password auditing and recovery application http://stake.com/research/lc/download.html (download link) • pwdump3 Windows NT/2000 remote password hash grabber http://www.polivec.com/pwdumpdownload.html (download link)
Control objective	Must have strong password policy in place. Systems must be configured to force all passwords to meet the complexity requirements. To enhance security, different passwords should be used on each server in a workgroup or domain. The Administrator account password must contain at least one non-alphanumeric character in the first seven characters.
Risk	Inadequate account and password policies, permitting the use of weak passwords. Weak passwords are easy to guess, simple to derive, and vulnerable to dictionary attack. Password hacking freeware are readily available that will do the job for the hackers, making a denial of service attack possible or gaining unauthorized access to proprietary information.
Likelihood	High
Consequence	Potential loss of system availability and integrity, should the compromised account have privileged permissions to the network. Unauthorised access to confidential corporate data.
Compliance/ Expected Results	• Password length must be set to at least 8 characters long, must expire at least every 60 days, must enforce password history, and password complexity requirements must be enabled. By default, all these settings are not defined. • To complement the system settings, a current internal logon account and password policy is in place.
Testing	1) From the auditor workstation, create an audit MMC. Click Start | Run, enter mmc and click OK. 2) From the Console menu, select 'Add/Remove Snap-in'. 3) From the list of available Standalone Snap-ins, select

'Security Configuration and Analysis' and click Add.
4) Repeat steps 2-3 for adding the Security Templates
    snap-in.
5) Click OK to close the 'Add/Remove Snap-in' window.

6) Expand the 'Security Templates' node to display all the
    templates within.
7) Highlight the 'basicwk' security template, select 'Action |
    Save As' and name the new template 'audit'.
8) Expand the 'audit' template and Account Policies node.
9) Select the 'Password Policy' node.

Modify the password policies as follow.
10) Set Enforce password history to 5 passwords
    remembered.
11) Set Maximum password age to 60 days
12) Set Minimum password age to 1 days
13) Set Minimum password length to 8 characters
14) Enable 'Passwords must meet complexity requirements'
15) Highlight the 'audit' template, select Action | Save As to
    re-save the 'audit' template with the changes made.
16) Right-click the 'Security Configuration and Analysis'
    scope item, and select Open Database.
17) Save the database as 'audit.sdb'.
18) Click Open
19) Right-click the 'Security Configuration and Analysis'
    scope item again, and select 'Import Template…'.
20) From the Import Template window, select the 'audit.inf'
    template and click Open to import the template into the
    database.

21) From the Action menu, select Analyze Computer Now. Accept the default location for the log file.
22) Once the analysis is finished, expand the 'Security Configuration and Analysis' scope item to view the results of the analysis.

Policy	Database Setting	Computer Setting
Enforce password history	5 passwords remembered	5 passwords remem…
Maximum password age	60 days	60 days
Minimum password age	0 days	0 days
Minimum password length	8 characters	8 characters
Passwords must meet complexity req…	Enabled	Enabled
Store password using reversible encr…	Disabled	Disabled

23) Look for red X's, which are system settings that deviate from the database settings.
24) From the Console menu, select 'Save' and name it 'audit.msc'. Close the MMC console.
25) For convenience of future use, send a shortcut of the file to the desktop.
26) Document the findings and attach screenshots to the report.
27) Further test can be done to discover all weak passwords on the domain, using a combination of the LC4 password auditing and pwdump3 password hash grabber tools. Both tools need to be downloaded and files extracted/installed beforehand.
28) From the auditor's workstation:
   - From the command prompt, from the pwdump3 program folder, run "pwpump3 <machinename of domain controller> <output filename>"
   - run LC4, and from the 'Get Encrypted Password' screen, select 'Retrieve from a remote machine'
   - click Next
   - choose the 'Custom' auditing method
   - click the 'Custom Options…' button

- select the top two options,
- ensure the 'brute force attack' option is not selected, as it is not required for this audit
- click OK to continue
- accept the default 'Pick Reporting Style' settings and click Next to continue
- click Finish to continue
- at the 'Import From Remote Registry' screen, click Cancel to continue

- click OK at the warning message
- from the Import menu select 'Import From PWDUMP File' and specify the output filename generated from running pwpump3.

- From the Session menu select 'Begin Audit'. It might take a while (5 minutes or more), depending on the number of user accounts in the domain that's being audited.
- On completion, from the File menu export the session to a text file for further analysis.

Stimulus/Response Test:
1) From the auditor's workstation, press Ctrl+Alt+Del.
2) Select Change Password….
3) Enter the old password followed by the new password and click OK.
   - For the new password, first enter '+Abc4' as the new password, which satisfies the complexity requirement but fails the minimum length requirement.
   - Secondly, enter 'abc4567890' as the new password, which satisfies the minimum length requirement but fails the complexity requirement.
   - In both cases, assuming the minimum length policy is set to 8, the following error message will be displayed.

   - Thirdly, enter '(S4v4nw0nd4rs)' as the new password (assuming this password has not been used during recent time), which satisfies all three requirements of password history, length and complexity. The system should accept it as a valid password.
4) Gather evidence of a current internal logon account and password policy.
5) Attach screenshot and document findings in audit report.

| Objective/ | Objective |

Subjective	

Test Results	• There are appropriate settings for the Password Policy.
	
	• Using the LC4 password auditing tool, a significant number of weak passwords have been found. Although these passwords conform to Microsoft's password complexity standards, they failed the LC4 Dictionary and Hybrid password cracks. The common thing among the weak passwords is the use of simple variations of familiar words, e.g., 'Tiger123'. For confidentiality reasons, output from LC4 cannot be attached to this report.
	• Various tests were performed to verify the password complexity requirements.
	    • Change password to '+Abc4', which fails the minimum length requirement. An appropriate warning message was displayed.
	    "Your password must be at least 8 characters; cannot repeat any of your previous 5 passwords; must contain capitals, numerals or punctuation; and cannot contain your account or full name. Please type a different password. Type a password which meets these requirements in both text boxes."
	    • Change password to 'abc4567890', which fails the complexity requirement. Again, an appropriate warning message was displayed.
	    • Change password to '(S4v4nw0nd4rs)', which meets all the requirements. The system accepted the new password.

Auditor Notes	Compliance test passed. However, a considerable number of users are using passwords that can be easily cracked by well-known password auditing tool such as LC4. It is recommended that users be reminded on a regular basis about what constitutes a good password. Although a current Network Logon Account and Password policy is in place, there is no indication that the Administrator account password must contain at least one non-alphanumeric character in the first seven characters.

Audit #7 – GPOs for Securing the Domains and Domain Controllers

Reference	• Internal documentation on group policies for Domains, Domain Controllers. • Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I". Version 1.0 (Chapter 4, *Tables 12-16, 29-30*) http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link)
Control objective	Availability, stability and integrity of the AD infrastructure must be maintained. Must secure the core components of the AD by implementing appropriate group policies for Domains and Domain Controllers.
Risk	Domains and Domain Controllers not secured by appropriate GPO settings.
Likelihood	High
Consequence	Incorrectly configured GPOs could open up security holes to the AD and the internal network. This could have adverse impact on the stability, integrity and availability of the AD.
Compliance/ Expected Results	• Appropriate group policies have been implemented for the Domains in following categories of policy settings: (1) password policy, (2) account lockout policy and (3) Kerberos policy. • Appropriate group policies have been implemented for Domain Controllers in the following categories of policy settings: (1) audit policy, (2) user rights assignment, (3) security options, and (4) event log.
Testing	1) Assume you have completed Check #6. 2) From the auditor workstation, open the 'audit.msc' MMC created in Check #6. Domains 3) Highlight the 'Security Templates' and expand the 'audit' node.

4) Apply best practice policy settings to Account Policies - Password Policy, Account Lockout Policy, and Kerberos Policy.

5) Right-click on the 'audit' template and select 'Save As…' to re-save the 'audit' template.
6) Right-click the 'Security Configuration and Analysis' scope item, and select 'Import Template…'.
7) From the Import Template window, select the 'audit.inf' template.
8) Click Open to import the template into the database.
9) From the Action menu, select Analyze Computer Now. Accept the default location for the log file.
10) Once the analysis is finished, expand the 'Security Configuration and Analysis' scope item to view the results of the analysis.

11) Expand each category of policy under 'Account Policies'.
12) Look for red X's, which are system settings that deviate from the database settings.
13) From the Console menu, select 'Save' to re-save the 'audit.msc' console.

Domain Controllers (complete this test in conjunction with the system administrator)
1) From the auditor/administrator workstation run 'Active Directory Users and Computers'.
2) Right-click the Domain Controllers OU.
3) Select 'Properties'.
4) Select the 'Group Policy' tab.

5) With the 'Default Domain Controllers Policy' highlighted, click 'Edit'.
6) Expand 'Computer Configuration | Windows Settings | Security Settings | Local Policies'.
7) Verify that the settings for 'Audit Policy', 'User Rights Assignment' (particularly 'Log on locally' and 'Shut down the system' policies), and 'Security Options' conform to best practice settings for Domain Controllers.
8) Repeat step (7) for 'Event Log | Settings for Event Logs'.

9) Document the findings and attach screenshots to the

	report. *Stimulus/Response Test:* <u>Domains</u> 1) Check #6 is one of the tests for the Domain policies. Another test could be completed on the 'Account Lockout Policy' using an account provided by the system administrator. Verify that the account gets locked out after a number of failed logon attempts, using a wrong password. <u>Domain Controllers</u> 2) Working in conjunction with the system administrator, verify that a general user account cannot log on locally to the Domain Controller. 3) Attach screenshots and document findings in the audit report.
Objective/ Subjective	Objective
Test Results	<u>Domain</u> • The Password Policy has been discussed in Audit #6. • The Account Lockout Policy and Kerberos Policy have both been implemented correctly. <u>Domain Controllers</u> • The 'Log on locally' policy setting does not conform to Microsoft's recommended setting.
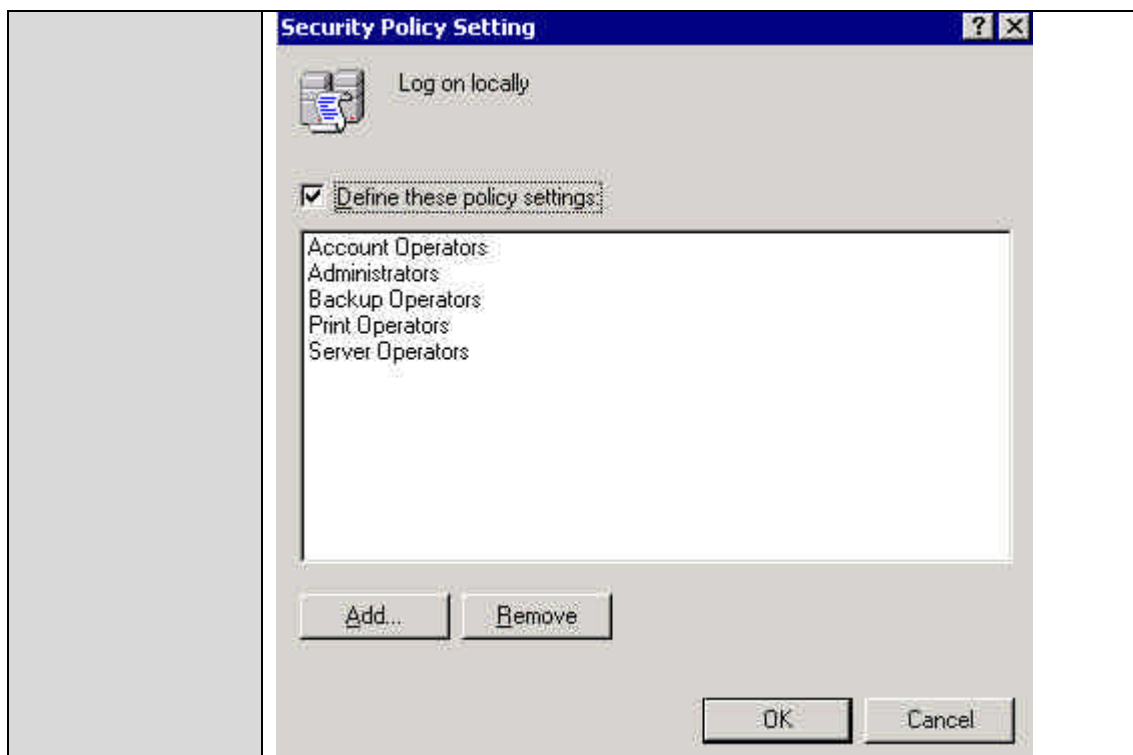
Security Policy Setting

Log on locally

☑ Define these policy settings

Account Operators
Administrators
Backup Operators
Print Operators
Server Operators

Add...   Remove

OK   Cancel

- The 'Shut down the system' policy setting does not conform to Microsoft's recommended setting.

Security Policy Setting

Shut down the system

☑ Define these policy settings

Account Operators
Administrators
Backup Operators
Print Operators
Server Operators

Add...   Remove

OK   Cancel

- The 'Auditing Policy' settings do conform to Microsoft's

recommended settings. (although the settings do more than what Microsoft have recommended)
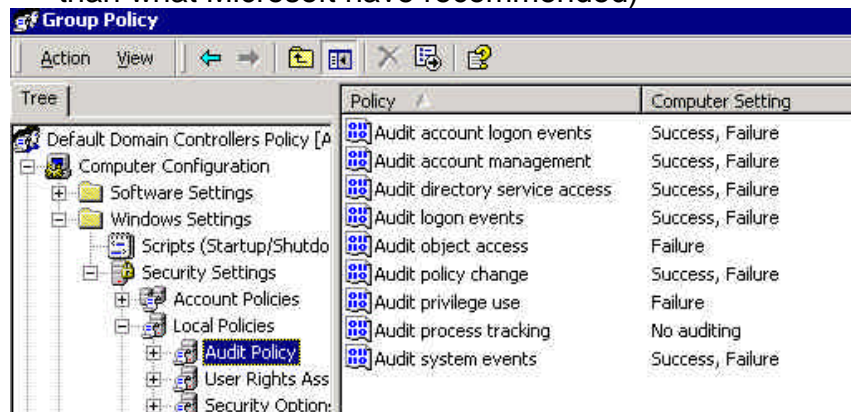
- The 'Security Options' policy settings do not conform to Microsoft's recommended settings. The following screenshot contains a subset of the policy settings.
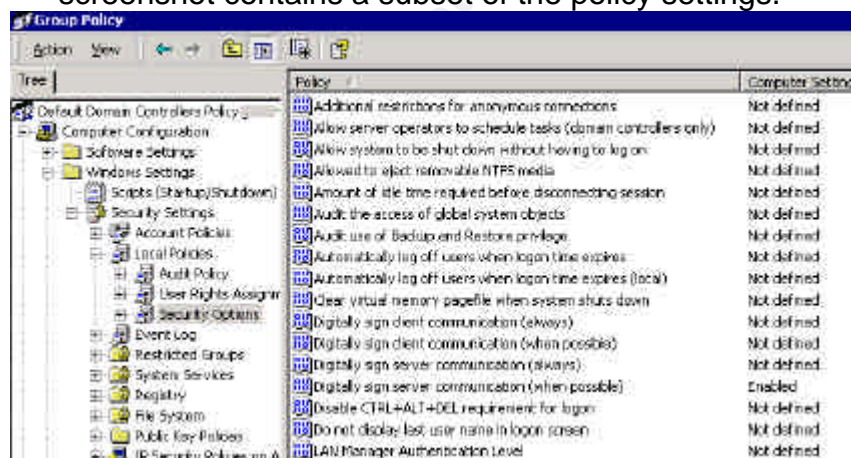
- The 'Event Log' policy settings do conform to Microsoft's recommended settings, and a further step has been taken to ensure the Domain Controllers do not shut down when the security audit log is full. The security log should not be full since the 'retention method for security log' policy is set to 'overwrite events as needed'.
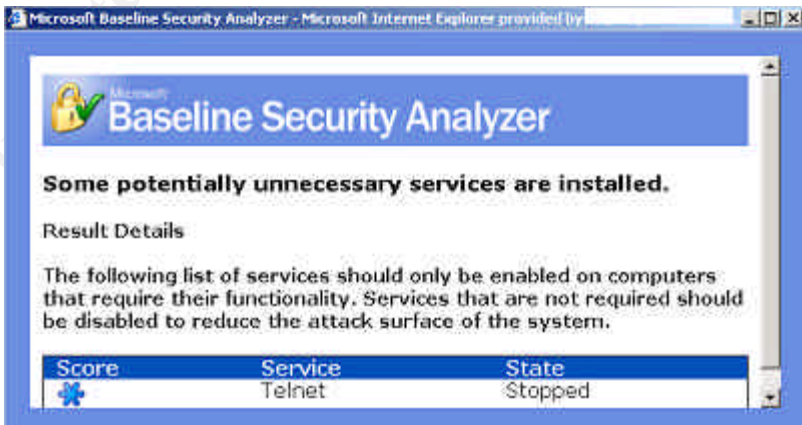
	• When a general user account is used to logon to the Domain Controller, the following error message is displayed. **Logon Message** ✕ ⚠ The local policy of this system does not permit you to logon interactively. [OK]
Auditor Notes	Compliance test failed for the Default Domain Controllers Policy. Significant changes need to be made to the following groups of policies in order to secure the Domain Controllers. • 'Log on locally' policy setting • 'Shut down the system' policy setting • 'Security Options' policy settings

Audit #8 – Services

Reference	• Microsoft Baseline Security Analyzer (MBSA) http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP (download link) • Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I". Version 1.0. (Chapter 3, *Table 9*) http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link) • SomarSoft Utilities. DumpSec http://www.somarsoft.com/ (download link)
Control objective	System integrity and availability must be maintained. Some services that have known security issues like, IIS, RAS and Terminal Services, must be reviewed and carefully configured. Network services that are not required for the server role must be disabled, in particular, the IIS components.
Risk	Unused/unnecessary services not disabled on the AD servers/Domain Controllers.
Likelihood	High
Consequence	Services that are installed by default but rarely used can contain widely exploited flaws that will put the operating system at risk.
Compliance/ Expected Results	Unnecessary services are disabled on the Domain Controllers. Common services to disable on Domain Controllers are: • Application Manager • ClipBook • Distributed Link Tracking • Distributed Transaction Coordinator • Fax Service • FTP Publishing Service (unless using for web hosting) • Indexing Service • IIS Admin Service (unless using for web hosting) • Internet Connection Sharing • License Logging Service • NetMeeting Remote Desktop Sharing • Print Spooler • QoS RSVP • Remote Access Auto Connection Manager • Remote Access Connection Manager

	• Routing and Remote Access • Telephony • Telnet • Utility Manager

Testing	1) Download and install MBSA.
	2) Run MBSA to scan the AD servers.
	3) From the security report locate the Additional System Information section.
	4) For the 'Services' issue, click 'Result details'.
	
	Additional System Information
	
	5) By default, this only scan for the following services, but the configurable list of services to be checked can be modified:
	    MSFTPSVC (FTP)
	    TlntSvr (Telnet)
	    W3SVC (WWW)
	    SMTPSVC (SMTP)
	
	6) Investigate the list of potentially unnecessary services that are installed on the AD servers. They should be disabled.
	
	7) Attach screenshots and document findings in the audit report.
	8) For a thorough audit of the services, use the SomarSoft DumpSec utility to obtain a complete list of services installed on the servers.
	9) Download and install the SomarSoft DumpSec utility.

10) Run DumpSec from the auditor workstation.
11) From the 'Report' menu select 'Select Computer…'.

12) Enter the name of the Domain Controller to be audited and click OK.
13) From the 'Report' menu select 'Dump Services…'.

14) On the 'Options for Services/Drivers Report' screen uncheck the 'Kernel drivers' selection box.

15) Click OK to continue.
16) On completion, click File | Save Report As…

17) Save the output file to an appropriate file type, this can then be imported into a spreadsheet or database for further analysis.

18) Analyze the output file for unnecessary services for the Domain Controller role.
19) Document the findings in the audit report.

Objective/ Subjective	Objective

Test Results	• The AD Domain Controllers that have been audited are all dedicated Domain Controllers with one exception, the Exchange 2000 bridgehead Server. However, all of them have the following unnecessary services running, for the role of a Domain Controller in the context of *The Company*.
	     o Distributed Link Tracking Client
	     o Distributed Link Tracking Server
	     o Distributed Transaction Coordinator
	     o License Logging Service
	     o Print Spooler
	     o Remote Access Connection Manager
	     o Telephony

	○ Application Management (on two of the Domain Controllers) ○ IIS Admin Service (on two of the Domain Controllers, but only the Exchange 2000 bridgehead Server needs this service running) ○ World Wide Web Publishing Service (on the Exchange 2000 bridgehead Server) • Attached is the screenshot of a part of the output file generated from the Somarsoft Dumpsec Utility. .txt - Notepad File Edit Format Help 26/04/2003 5:37 p.m. - Somarsoft DumpSec (formerly DumpAcl) - \\TestDC FriendlyName Name Status Type Account Alerter Alerter Running Win32 LocalSystem Altiris Client Service AClient Running Win32 LocalSystem Application Management AppMgmt Running Win32 LocalSystem Automatic Updates wuauserv Running Win32 LocalSystem Background Intelligent Transfer Service BITS Stopped Win32 LocalSystem ClipBook ClipSrv Stopped Win32 LocalSystem COM+ Event System EventSystem Running Win32 LocalSystem Compaq Event Notifier CIMNotify Stopped Win32 LocalSystem Compaq Foundation Agents CqMgHost Running Win32 LocalSystem Compaq NIC Agents CPQNicMgmt Running Win32 LocalSystem Compaq Remote Monitor Service CpqRcmc Running Win32 LocalSystem Compaq Server Agents CqMgServ Running Win32 LocalSystem Compaq Storage Agents CqMgStor Running Win32 LocalSystem Compaq Version Control Agent cpqvcagent Running Win32 LocalSystem Compaq Web Agent CpqWebMgmt Running Win32 LocalSystem Computer Browser Browser Running Win32 LocalSystem DefWatch DefWatch Running Win32 LocalSystem DHCP Client Dhcp Running Win32 LocalSystem DHCP Server DHCPServer Running Win32 LocalSystem Distributed File System Dfs Running Win32 LocalSystem Distributed Link Tracking Client TrkWks Running Win32 LocalSystem Distributed Link Tracking Server TrkSvr Running Win32 LocalSystem Distributed Transaction Coordinator MSDTC Running Win32 LocalSystem DNS Client Dnscache Running Win32 LocalSystem DNS Server DNS Running Win32 LocalSystem Event Log Eventlog Running Win32 LocalSystem Fax Service Fax Stopped Win32 LocalSystem File Replication Service NtFrs Running Win32 LocalSystem hp ProLiant System Shutdown Service sysdown Running Win32 LocalSystem IIS Admin Service IISADMIN Running Win32 LocalSystem Indexing Service cisvc Stopped Win32 LocalSystem • A complete output file generated from the Somarsoft Dumpsec Utility, for one of the Domain Controllers, is attached in *Appendix B* for reference.
Auditor Notes	Compliance test failed.

Audit #9 – DNS

Reference	• Microsoft. "Security Operations Guide for Windows 2000 Server". Chapter 3 - Managing Security with Windows 2000 Group Policy http://www.microsoft.com/downloads/details.aspx?FamilyID=f0b7b4ee-201a-4b40-a0d2-cdd9775aeff8&DisplayLang=en (download link) • DcDiag.exe: Domain Controller Diagnostic Tool, • NetDiag.exe: Network Connectivity Tester, From Microsoft Windows 2000 SP3 Support Tools http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/supporttools.asp (download link)
Control objective	The loss of the DNS must be prevented because it is used by the AD to locate services on other hosts that network users may rely on. Must prevent unauthorized users from exploiting it as a means of gaining access to the AD.
Risk	Failure of the DNS
Likelihood	High
Consequence	The AD service will fail to locate network resources.
Compliance/ Expected Results	• No errors should be reported by the running of the AD support tools: dcdiag and netdiag. • Access (physical as well as remote access) to the Domain Controllers is restricted based on the administrative roles and responsibilities for the AD.

Testing	1) Perform this test in conjunction with the system administrator.
	2) Install the Windows 2000 SP3 Support Tools.
	3) Provide the system administrator with a floppy disk (or CD) containing DcDiag.exe and NetDiag.exe.
	4) Run the tools on each Domain Controller in each Domain or have a batch file for scanning all the Domain Controllers in each Domain. Both tools are to be run from the command prompt.
	5) The command line for DcDiag.exe is:
	  • Dcdiag */s:DomainController* /u:*Domain\UserName* /p:* /f:*outputfilename.Log*
	  • (username is the user account of the administrator)
	6) The command line for NetDiag.exe is:
	  • Netdiag /d:*DomainName* > *outputfilename.Log*
	7) If there are errors found in the output files, rerun the same commands with the additional /v (verbose) flag to generate output with extended information.
	8) Repeat the physical and remote access tests in Audit #1. (page 77-79)
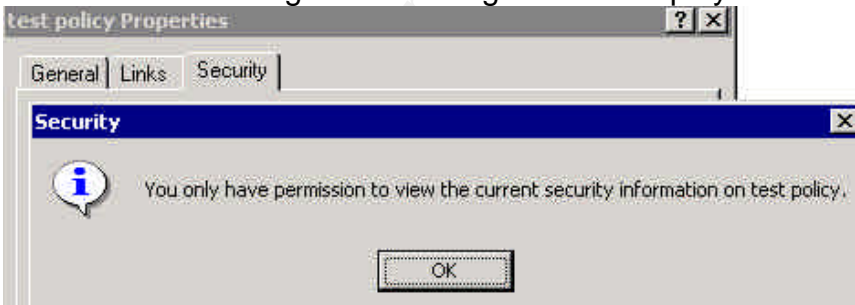
	9) Document the findings in the report.
Objective/ Subjective	Objective

Test Results	• DcDiag.exe ran successfully.
	• One of the Domain Controllers failed the 'systemlog' test. Attached is the error message.
	
	Starting test: systemlog
	  An Error Event occured. EventID: 0xC00010DF
	    Time Generated: 04/26/2003 13:10:25
	    Event String: A duplicate name has been detected on the TCP
	     An Error Event occured. EventID: 0xC00010DF
	    Time Generated: 04/26/2003 13:34:30
	    Event String: A duplicate name has been detected on the TCP
	    .... TestDC1 failed test systemlog
	
	• Request the system administrator to rerun DcDiag with the –v flag for an extended output.
	• 'DcDiag.Log', the complete output file from one of Domain Controllers, is attached in *Appendix C* for reference.
	(Require the right version of DcDiag.exe for this to work. I used the copy of DcDiag.exe dated 11/01/2002. The latest version of DcDiag.exe does not work for me.)
	
	• NetDiag.exe ran successfully.
	• One of the Domain Controllers failed the DNS test. Attached is the error message.
	
	DNS test . . . . : Failed
	  [WARNING] The DNS entries for this DC are not registered correctly on DNS server 'x.x.x.x'. Please wait for 30 minutes for DNS server replication.
	  [WARNING] The DNS entries for this DC are not registered correctly on DNS server 'x.x.x.x'. Please wait for 30 minutes for DNS server replication.
	  [FATAL] No DNS servers have the DNS records for this DC registered.
	
	• Request the system administrator to rerun NetDiag with the –v flag for an extended output.
	• The complete output file, 'NetDiag.Log', is attached in *Appendix D* for reference.
	• Refer to the test results in Audit #1 for the physical and remote access tests. (page 77-79)

Auditor Notes	Compliance test failed.

Audit #10 – GPOs Security

Reference	• netiQ. Securely Managing Your Group Policies. White Paper, 11 March 2002. http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf
Control objective	Availability, stability and integrity of the AD infrastructure must be maintained. The ability to modify group policies must be restricted to a limited number of administrators. Changes to the group policies must follow the Change Control Management process. Must be able to back up and restore all or selective GPOs. To enhance security and provide redundancy for quick disaster recovery, offline storage of policy settings through templates must be considered.
Risk	Responsibilities for the management of GPOs not clearly defined. By default, all 'Domain Admins' of a child domain can modify group policies within that domain. And, some backup software runs as a Windows 2000 Service and needs to be a member of 'Domain Admins' for it to work. Such service accounts, once their passwords are discovered, are an alternative source for gaining unauthorised access to the GPOs. Changes to group policies not implemented in a controlled manner. GPOs and/or system state of all AD Domain Controllers not backed up and restore not tested.
Likelihood	High
Consequence	Group policies that are incorrectly configured and applied could open up security holes to the AD and the internal network. For example, allowing anonymous logon and having passwords that never expire, allowing Everyone/Full Control access permissions on file shares, and having unnecessary members in the Administrators and Guest user groups. Group policy changes that are not properly managed can produce unexpected results in the user environment, and affect the integrity and availability of the AD infrastructure. They also make troubleshooting difficult. Using the default settings, the larger the number of 'Domain Admins', the more difficult it is to establish accountability for group policy changes, and maintain the integrity and stability of the AD. Disaster recovery is impossible without successful backup

	of the AD Domain Controllers and GPOs.
Compliance/ Expected Results	• Responsibilities for the GPOs are clearly defined and understood by the system and security administrators. • Change Control Management procedures are followed for changes made to the group policies. • Restrictions have been applied to GPOs to allow only a specific group of administrators the ability to 'edit' the GPOs. For example, only the 'Enterprise Admins' and 'GPO Admins' user groups are granted the following permissions on all or selected GPOs, the OU that contains the GPOs, and the 'GPO Admins' user group object. - Write - Create All Child Objects - Delete All Child Objects The general 'Domain Admins' would then have Read only permissions on GPOs, GPOs OU, and the 'GPO Admins' objects in the AD. This is particularly useful when the 'Domain Admins' user group contains a wide range of user accounts, including service accounts of server backup software, for example, that are running on the AD Domain Controllers. It is advisable to centralize the GPOs in an OU.
Testing	1) Gather evidence that the responsibilities for the GPOs are clearly defined and understood by the system and security administrators. This can be achieved by acquiring the necessary documentation relating to the AD infrastructure, roles and responsibilities for AD, and interviewing key security and/or system administrators. If necessary, interview the Security Directory or equivalent. 2) Gather evidence that changes made to the group policies are clearly and fully recorded in the Change Control database. Request for a report from the Change Control database, for all group policy changes that occurred in the last three months. Verify the changes with some of the audits carried out in this assignment. 3) Gather a list of GPOs from the security and/or system administrator. 4) Analyze the permissions assigned to the GPOs. 5) Analyse the permissions assigned to the GPO OU, if
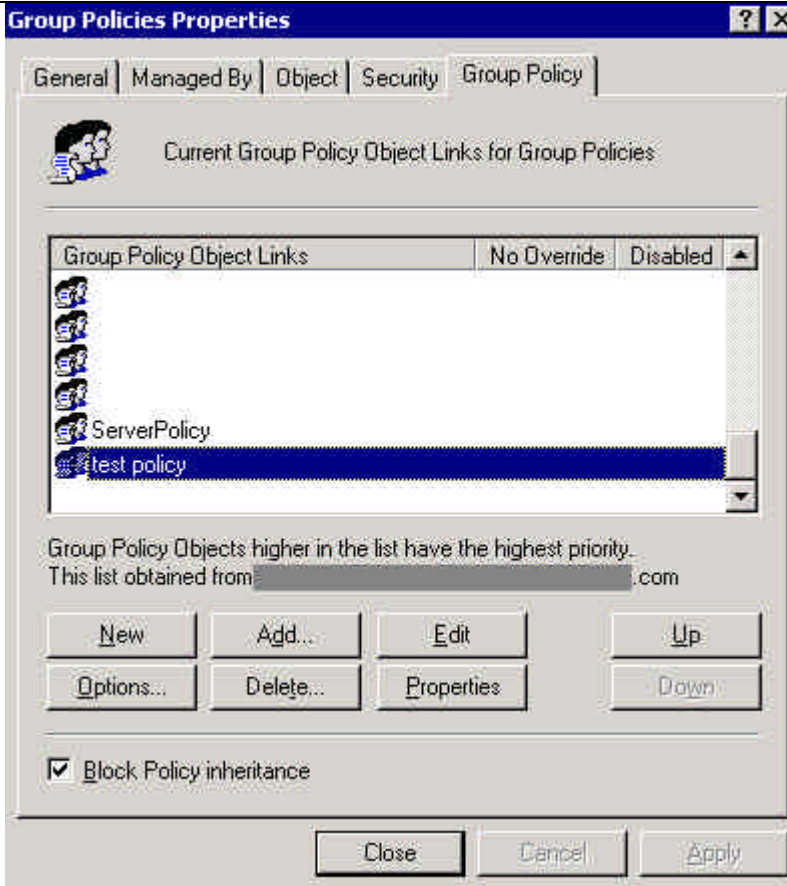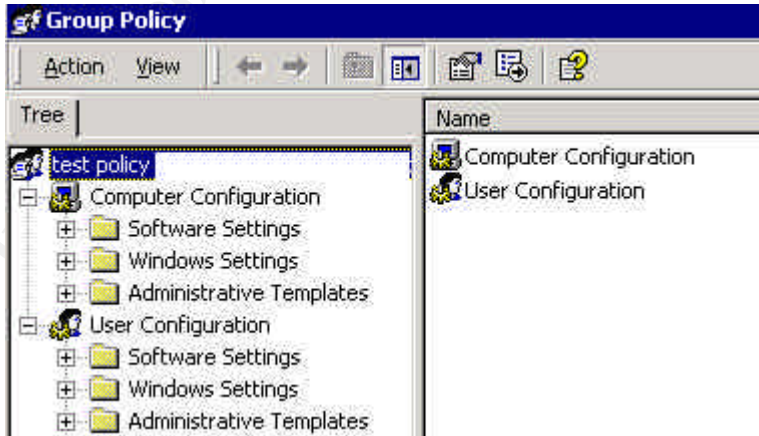
	exist.
	6) Analyse the permissions assigned to the 'GPO Admins' or equivalent user group, if exist. (consult the administrator, if necessary)
	Stimulus/Response Testing:
	1) Request one of the administrators, who have been restricted from modifying group policies, to logon to the AD domain controller.
	2) From 'Active Directory Users and Computers', locate one of the restricted GPOs.
	3) In the 'Group Policies Properties' window, highlight a restricted GPO and confirm that the 'Edit' button is dimmed for the particular GPO.
	4) With the restricted GPO still highlighted, click the 'Properties' button.
	5) In the 'xx Policy Properties' window, select the 'Security' tab. The following error message should display.
	6) Attach screenshots and document findings in the audit report.
	7) By default, all 'Domain Admins' and 'Enterprise Admins' have the permissions to modify group policies.
	8) Attach screenshot and document findings in the audit report.
Objective/ Subjective	Objective
Test Results	• There was evidence of clearly defined and documented roles and responsibilities for the management of the AD, which include the GPOs.
	• An audit of the Change Control database indicated that the Change Control procedure has been followed for AD/GPOs related changes.
	• An audit of the GPOs revealed that the default permissions apply, that is, 'Domain Admins' and 'Enterprise Admins' can modify all GPOs, and the GPO OU.

- A 'GPO Admin' or equivalent use group did not exist.
- Attached is the screenshot of the security settings for one of the GPOs.
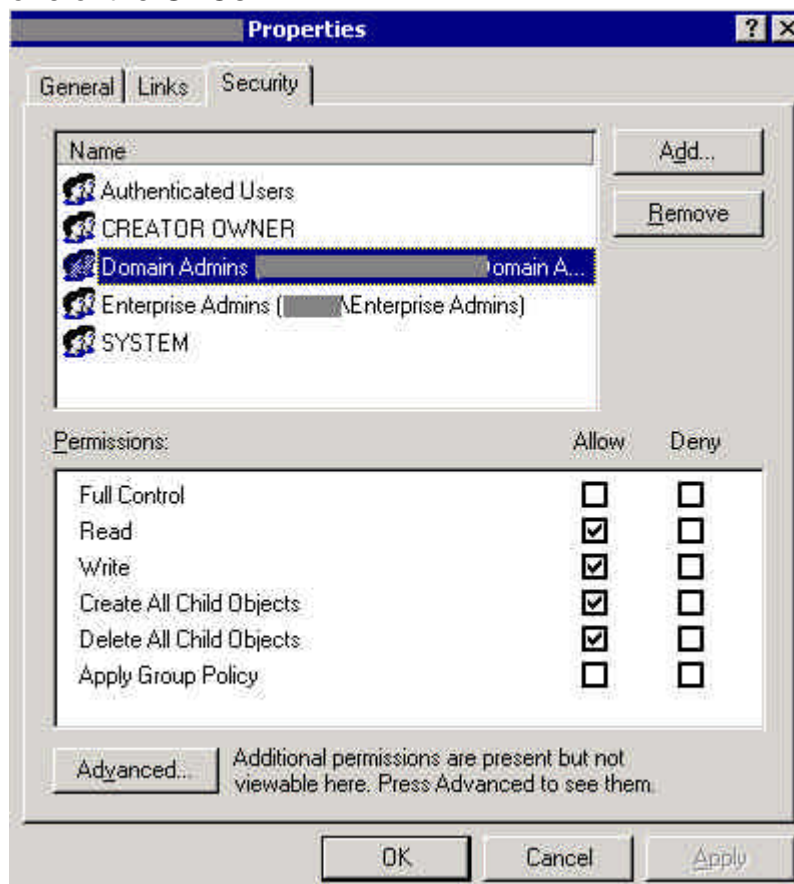
- Administrator-x who was not responsible for the maintenance of GPOs had been asked to logon and run 'Active Directory Users and Computers'.
- Within the 'Group Policies' OU Administrator-x was able to create/modify a new GPO. In this case, the new GPO was called 'test policy'.

	Group Policies Properties ? X
	
	General | Managed By | Object | Security | **Group Policy**
	
	Current Group Policy Object Links for Group Policies
	
	| Group Policy Object Links | No Override | Disabled ▲ |
	
	ServerPolicy
	test policy
	
	Group Policy Objects higher in the list have the highest priority.
	This list obtained from ███████████.com
	
	New Add... Edit Up
	Options... Delete... Properties Down
	
	☑ Block Policy inheritance
	
	Close Cancel Apply
	
	Group Policy
	Action View ← → 🔲 🔳 📑 📑 📑
	
	Tree | Name
	test policy
	  Computer Configuration
	    Software Settings
	    Windows Settings
	    Administrative Templates
	  User Configuration
	    Software Settings
	    Windows Settings
	    Administrative Templates
	
	Computer Configuration
	User Configuration

Auditor Notes	Compliance test failed.

Measure Residual Risk

There is strong perimeter defence against external attacks. Internally, *The Company* has exercised tight physical security controls, although a small number of temporary access cards were found to have unauthorised access to the Computer Rooms. A strong governance model exists, and well-developed processes and procedures have been put in place, to meet the demanding service requirements of a 24x7 business.

The IT Management Team is highly aware of network and systems security issues, and is committed to enabling business continuity by providing a secured and robust IT environment.

The majority of the control objectives have been met during this audit. However, a small number of significant weaknesses exist that will require a fair amount of effort, if the control objectives in those areas are to be met. The most significant risk to *The Company* uncovered by this audit is that not all the AD Domain Controllers have been backed up. This means it is not possible to recover the AD should a catastrophe occur to the AD. It is apparent that inadequate skills are available internally for the support of the new backup system. This problem is now given top priority to be resolved. Together with the backup issue, most of the weaknesses discovered in this audit can be fixed, with the following exceptions.

Vulnerability	Exposure to known security threats in Windows 2000.
Control Objectives	Exposure to published security threats must be minimized, by the timely implementation of Service Packs and hotfixes. New Service Packs and hotfixes must be implemented in a controlled manner. The risk of implementing any inappropriate hotfixes must be minimized.
Residual Risk	Lack of priority and/or resources given to meeting the control objectives, as daily operations requirements always come first.
Recommendation	The Management Team must ensure that the Security Patch Management Process that has been put in place, is adhered to by all administrators. If resource constraint is a real issue, the (actual) implementation of new Service Packs and hotfixes could be automated using a tool such as Software Update Services (SUS) from Microsoft, although the approval process must remain a manual process. In addition, a new Service Pack or hotfix must be tested before its implementation in the production network, as documented in the current Security Patch Management Process.

	Restrict the use of any automated tool like the SUS to a limited number of appropriately trained administrators.
Estimated Costs (assuming the automated tool is SUS)	<u>Setup Costs</u> Software = $0 Hardware = $0, using existing software deployment server External labour, 16 hours @$185 an hour → $3000 (round up) Or internal labour, 24 hours @$40 an hour → $1000 (round up) Total labour cost = between $1000 and $3000 <u>Ongoing Costs</u> Associated costs in maintaining and auditing the validity and appropriate use of the automated tool. Considering the costs of recovering from a Denial of Service attack to the network and/or the AD Domain Controllers, it should be justifiable to implement an automated tool such as the SUS; if that would help in keeping all Domain Controllers and Servers up-to-date with the latest Service Packs and hotfixes.

Vulnerability	Over reliance on external resources.
Control Objectives	To maintain a team of highly skilled administrators internally.
Residual Risk	Potentially adverse impacts on response time, knowledge transfer, accountability, system availability, and total cost of ownership in the long run. In addition, extensive utilization of external resources, especially if they are from a wide range of different sources, would make it difficult to adequately protect the security of proprietary information.
Recommendation	Hire additional permanent resource.
Estimated Costs	Software = $0 Hardware = $0 Additional labour, @$65,000 per annum, per qualified administrator.

Vulnerability	Unauthorised access to the AD and intellectual corporate data, should the compromised accounts have privileged permissions to the network/AD.
Control Objectives	To enforce the use of strong passwords for all user and administrative accounts.
Residual Risk	It is possible to have a weak password that passes the Password Complexity Requirements test. The Password Complexity Requirements require a password to meet at least three of the following four conditions: • Upper case • Lower case • Numbers • Non-alphanumeric characters Hence 'Password1', a relatively weak password, will be accepted by the system for passing the Password Complexity Requirements test.
Recommendation	Ongoing and regular user education on the use of strong passwords, until Microsoft has come up with a better Password Complexity Requirements test.
Estimated Costs	Software = $0 Hardware = $0 Internal labour, @$40 an hour, on an ongoing basis, until a better tool is available for the enforcement of strong passwords.

Evaluate the Audit

The Windows 2000 Active Directory Infrastructure is auditable, although requiring considerable amount of time and cooperation from the internal administrators who are overloaded with operations tasks.

The majority of the audit objectives have been achieved. However, within the scope of this audit it was not possible to determine whether security related processes, policies and procedures, have been effectively enforced by the Management Team. In particular, is everybody in the IT department fully aware of the processes, policies and procedures, do they adhere to them, and do all the IT Managers take responsibilities in making sure their staff adhere to them?

Freeware tools were readily available for completing the required audit tests, although there was a bit of a challenge gaining the appropriate access permissions to the entire system.

Assignment 4 – Audit Report

Executive Summary

I have completed an audit of *The Company*'s new Windows 2000 Active Directory infrastructure, which has been implemented at the Head Office.

The key objectives were to ensure that the confidentiality, integrity and availability requirements of the Active Directory infrastructure were met. This includes an analysis of the preventative measures, detective mechanisms and reactive guidelines that were in place to mitigate risks that could adversely impact the continuity of the Active Directory.

The core components of the Active Directory infrastructure were analysed to ascertain that the security design of the Active Directory is in line with the industry's best practices. Any weaknesses within the design and implementation of the Active Directory are highlighted in this report. They would need to be addressed before subsequent implementations at the branch offices. To insure consistency throughout the organization, it is important to assure that the implementations at the branch offices adhere to the security governance set at the Head Office.

This report sets out the key findings arising from the review of the Active Directory infrastructure which includes the security of the following core components.
- Active Directory Domain Controllers
- Delegation of administrative control of the Active Directory
- Restriction of administrative tools to authorised administrators
- Active Directory access controls
- Maintenance of Service Packs and hotfixes on the Domain Controllers
- Password security
- Security policy settings for Domains and Domain Controllers
- Services that are running on the Domain Controllers
- Security of the policy objects

This review was performed during April 2003. Any subsequent changes to the Active Directory, operating system security and configuration settings, or processes and procedures since that period, are outside the scope of this review.

Audit Findings

The following risks were discovered during the audit of the Windows 2000 Active Directory at *The Company*.

Finding 1 – Domain Controllers	
Reference: Audit #1, page 77	
Analysis	Findings
Tests were carried out on the following areas of concern: • Redundancy for the Domain Controllers • Remote Access • Physical Access	• There was evidence of redundancy for the Domain Controllers. • There were appropriate controls on remote access to the Domain Controllers. • The main concerns were around physical security, whereby some temporary access cards were found to have granted access to the computer rooms.
Risks (risk priority: critical) If the physical access to the Domain Controllers is compromised, which is highly possible due to the frequent use of temporary access cards, an attacker could cause physical damage to the Domain Controllers (and other Servers) rendering it unavailable. Or the Domain Controllers could be stolen. If password security were compromised at the same time, the attacker could gain unauthorised access to the Active Directory and proprietary information could be lost.	

Finding 2 – Active Directory Access Controls and ACLs	
Reference: Audit #4, page 88	
Analysis	Findings
Active Directory and file system access permissions were reviewed to uncover any inappropriate security settings.	• Default access permissions were found at the root of the logical disk volumes of Domain Controllers whereby *Everyone* were granted *Full Control*. • Default access permissions were also discovered on some of the file systems.
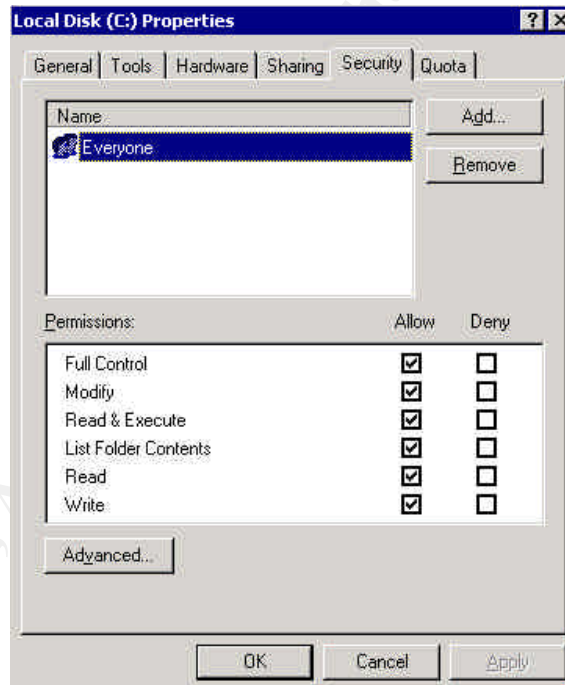
Risks (risk priority: critical)
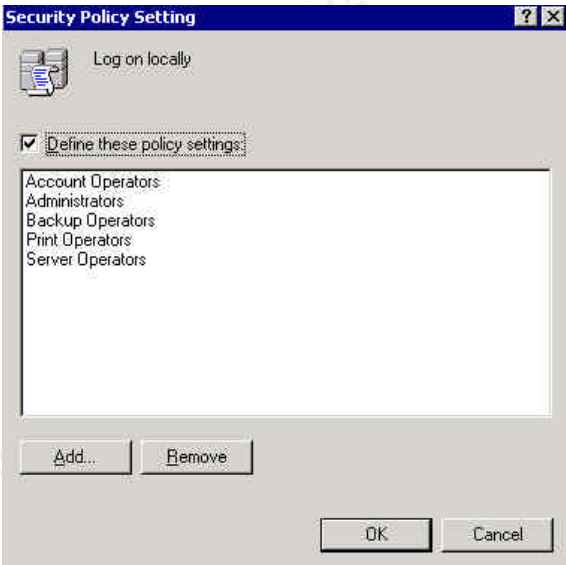
The default access permissions were deemed to be too permissive. With the current settings the Domain Controllers are vulnerable to disk-space attacks to the logical disk volumes. Incorrectly configured file systems are vulnerable to unauthorised access. For example, an attacker could use the authorised access to launch a Denial-of-Service attack to the particular system or the entire network.

A disk-space attack is also known as a resource starvation attack.

"For example, an attacker might continuously issue requests to your Web site to create baskets or create users. If this occurs, you will run out of disk capacity." (ref. http://msdn.microsoft.com/library/default.asp?url=/library/en-us/csvr2002/htm/cs_se_securecode_qiqw.asp)

Finding 3 – Service Packs and hotfixes	
Reference: Audit #5, page 92	
Analysis	Findings
The Domain Controllers were tested for the latest Service Packs and hotfixes.	• A patch management process was put in place but it was not strictly followed. • All Active Directory Domain Controllers were found to have missing hotfixes. • There was indication that the main causes for the outdated hotfixes were: lack of resources and low priority given by Management.
Risks (risk priority: critical)	
One of the key elements of running a secure system is to stay up to date with operating system software security patches that are released by the software vendor. At their present state, the Domain Controllers being audited are exposed to known security threats. Attackers can exploit the vulnerability to gain elevated privileges to the system and launch a Denial of Service attack or execute codes for gaining unauthorised access. In the case of a successful attack, the confidentiality of data would be compromised.	

Finding 4 – GPOs for Securing Domains and Domain Controllers	
Reference: Audit #7, page 100	
Analysis	Findings
Domains and Domain Controllers are key components of an Active Directory. Group policies are the mechanisms used to secure the key components. The default Domain and Domain Controllers Group Policies were tested against the industry's best practices and Microsoft's recommended settings.	• It was found that too many administrative parties were allowed to logon on locally and shut down the Domain Controllers. • The Security Options policy settings were not in line with Microsoft's recommended settings.

Risks (risk priority: high)

The stability and availability of the Active Directory Domain Controllers can be compromised with too many parties having the ability to <u>logon locally</u> or <u>shut down</u> the systems. Those are tasks that need to be completed in a controlled manner by appropriately skilled administrators.

If the password of the parties concerned is compromised an attacker will be granted the permission to logon locally to the Domain Controllers. From there the attacker will be able to run codes of his or her choice to launch an attack or gather more confidential information which will help make possible a future attack.

The Domain Controllers are subject to unauthorised usage if the <u>Security Options</u> are not configured appropriately. For example, the default setting permits a user who can logon locally to the Domain Controllers to install printer drivers, and perform disk-space attacks by submitting large print jobs.

Finding 5 – Services	
Reference: Audit #8, page 107	
Analysis	Findings
Based on the role of a Domain Controller, a review was completed of the services that were running on the Domain Controllers, to determine any unnecessary services that should be disabled.	• All the Domain Controllers have some unnecessary services running. These services should be disabled.
Risks (risk priority: critical) Services that are installed by default but rarely used can contain widely exploited flaws that will put the operating system at risk. One example is the IIS Admin Service which is <u>only</u> needed on a web hosting server. Hence it should be disabled on all Domain Controllers, as they are not web hosting servers.	

Finding 6 – DNS	
Reference: Audit #9, page 112	
Analysis	Findings

The access to the Domain Controllers, where the DNS configuration takes place, was reviewed.
The Domain Controller Diagnostic Tool (DcDiag) was used to produce output from which error events can be identified and investigated in order to mitigate the risk of corrupted DNS and Domain Controllers.
The Network Diagnostic tool (NetDiag) was used to produce output from which DNS errors can be identified and investigated.
	• One of the Domain Controllers audited, *TestDC1*, failed the 'systemlog' test as reported by DcDiag.
	
	Starting test: systemlog
	   An Error Event occured. EventID:
	0xC00010DF
	       Time Generated: 04/26/2003 13:10:25
	       Event String: A duplicate name has been
	detected on the TCP
	       An Error Event occured. EventID:
	       0xC00010DF
	       Time Generated: 04/26/2003 13:34:30
	       Event String: A duplicate name has been
	       detected on the TCP ....
	       TestDC1 failed test systemlog
	
	• A separate Domain Controllers, *TestDC2*, failed the DNS test as reported by NetDiag.
	
	DNS test . . . . : Failed
	   [WARNING] The DNS entries for this DC are not
	registered correctly on DNS server 'x.x.x.x'. Please
	wait for 30 minutes for DNS server replication.
	   [WARNING] The DNS entries for this DC are not
	registered correctly on DNS server 'x.x.x.x'. Please
	wait for 30 minutes for DNS server replication.
	   [FATAL] No DNS servers have the DNS records
	for this DC registered.

Risks (risk priority: critical) Unauthorised access to the Domain Controllers would give rise to unauthorised access to the DNS service. The DNS service must be configured by appropriately trained administrators. Should the DNS fail the Active Directory service will fail to locate network resources.	

Finding 7 – GPOs Security	
Reference: Audit #10, page 114	
Analysis	Findings
The security of the Group Policy Objects (GPOs) was reviewed, to verify who can modify them and how group policies changes are managed. Inappropriate changes to the GPOs will have adverse impact on the availability, integrity and stability of the Active Directory infrastructure. The backup and restore of GPOs is very important for quick disaster recovery, and hence was also reviewed.	• There was clear definition of the roles and responsibilities for the administration of the Active Directory. Changes relating to the GPOs were implemented according to the Change Control Management process. • However, there was no additional security measure in place for restricting changes to GPOs to specific administrators. Hence, by default any user account which is part of the 'Domain Admins' user group will be able to modify the GPOs.

Properties

General | Links | Security

Name
- Authenticated Users
- CREATOR OWNER
- Domain Admins   Domain A...
- Enterprise Admins ([   ]\Enterprise Admins)
- SYSTEM

Add...
Remove

Permissions:	Allow	Deny
Full Control	☐	☐
Read	☑	☐
Write	☑	☐
Create All Child Objects	☑	☐
Delete All Child Objects	☑	☐
Apply Group Policy	☐	☐

Advanced...   Additional permissions are present but not viewable here. Press Advanced to see them.

OK   Cancel   Apply

Risks (risk priority: high)
Unauthorised changes to the GPOs could take place by the use of user accounts, which are members of the 'Domain Admins'. Inappropriate changes to the GPOs could adversely impact the security, integrity and stability of the Active Directory infrastructure, including introducing new security holes. For example, an incorrect Security Options policy setting could enable a user who can logon locally to the Domain Controllers to install printer drivers, and launch a disk-space attack to the Domain Controllers by submitting large print jobs.

Finding 8 – Backup and Restore of Domain Controllers	
Reference: Check #25, page 72	
Analysis	Findings
The backup configuration and schedule for the Domain Controllers were reviewed, and backup logs were analysed. It was also verified whether a disaster recovery procedure for the Active Directory is in place and tested.	- Not all the Domain Controllers were being backed up. - Due to staff turnover the new administrator was in the process of getting to know the environment and rectifying item by item, systems that were not working to expectations. - Disaster recovery procedure for the Domain Controllers and Active Directory had not been fully documented and tested.
Risks (risk priority: critical) Unavailability of the entire Windows 2000 Active Directory for an extended period of time. It might not be possible to restore the Active Directory in the event of a disaster, since one of the Domain Controllers is not being backed up. Should a disastrous event occur at this point in time, it would be a huge task rebuilding the entire Active Directory infrastructure, from scratch, based on any documentation available at the time.	

Audit Recommendations

One of the key objectives of this audit is to provide practical recommendations for addressing the identified risks.

As part of the review it was identified that although sufficient controls and preventative measures exist, no automated intrusion detection mechanism is in place. Therefore, there is heavy reliance on the individuals to manually monitor the systems for any security issues. Often this is being omitted due to resource constraint in keeping up the operations of the systems.

Recommendations:

1. The physical access user matrix should be reviewed every two months. Permissions on all access cards should be validated every two months. The use of temporary access cards should be minimized. A photo ID card is preferable to the use of temporary access cards with no photos.

2. To counteract the risk of a resource starvation attack, for example, the disk space, default access permissions on the root of the logical disk volumes of Domain Controllers and new file shares should be modified after the initial installation and creation. To safeguard against a disk-space attack, a reasonably large file (10% of the usable disk space) should be created on the root of the logical disk volumes of Domain Controllers (and Servers) after the initial installation. A Server Setup and Configuration Checklist should be created to ensure all server installations and security configurations are in line with the industry's best practices.

3. Security patches released by Microsoft should be considered for implementation on all Domain Controllers and Servers as a company standard, and a record should be maintained of the current patch status. The use of an automated tool like SUS from Microsoft could be considered but must be carefully planned, configured and controlled, and used only if there were real resource issues.

   The Operations team should hold responsibility for the assessment and the day-to-day maintenance of server security patches and that the Security Administrator should perform regular and independent reviews of all the Domain Controllers and Servers.

   The Management Team should review the current priority given to keeping all Domain Controllers and Servers current with Service Packs and security patches, as an assurance to maintain the high availability of the Active Directory. Any resource issues should be recognised and rectified in a timely manner.

4. Group policies should be appropriately configured to be in line with the approved roles and responsibilities for the administration of the Active Directory and Domain Controllers. The ability to shut down and logon locally to the Domain Controllers should be limited to a designated group of system administrators. To enhance the security to the Domains and Domain Controllers, security options and the default Domain and Domain Controllers group policies should be reviewed after the initial installation and brought in line with the industry's best practices and Microsoft's recommended settings.

5. After the initial installation of the Domain Controllers the default services that are running should be reviewed and redundant services for the role of a Domain Controller should be disabled, before cutting over to production. This is another item that should be included in the Server Setup and Configuration Checklist.

6. To ensure the stability of the Active Directory infrastructure system administrators should run the Domain Controller and Network Diagnostic tools on a weekly basis, so that DNS and network related issues could be identified and addressed in a timely manner.

7. To further secure the Active Directory infrastructure, the ability to modify group policies should be limited to a designated group of 'GPO Admins' and the default 'Domain Admins' user group should be granted ReadOnly permissions on the Group Policy Objects.

8. As a matter of urgency the system administrators should be urged to add the missing Domain Controller into the backup job schedule. Apart from ensuring that the entire team of Domain Controllers is being backed up, the system administrators should ensure that the right backup type is being used. This is because Microsoft only supports FULL backup on Active Directory. The incremental and differential backup types are not recommended because they tend to have problems on the backing up of the Active Directory.

9. Systems administrators should review system logs on a daily basis as part of the day-to-day administration role. This is to ensure that system errors are identified early and resolutions put in place timely to minimize the risks of system corruptions and availability.

Costs (in NZ$)

The costs to fix the identified problems are mostly around internal resources. There are no additional software and hardware costs.

The estimated additional costs are:
- Potential one-off installation cost for SUS in both test and production networks, between $1000 and $3000,
- Potential ongoing cost for the maintenance and review of the SUS software @$40 an hour once a fortnight or $80 a month,
- Ongoing technical training for the systems and security administrators @$5,000 per head count, per annum,
- Ongoing end-user training provided by the IT department @$40 an hour,
- Ongoing review of system logs @$20 per half hour each day or $100 per week,
- Potential one-off cost of hiring an additional system administrator @$65,000 per head count, per annum.
- Notification system. Unknown, depending on requirements.

Compensating Controls

Technical training is important for the systems administrators but the costs could be reduced if online computer based training can be arranged, and made available to a large audience in the technical team.

The costs associated with the SUS software could possibly be eliminated by a management review of the existing technical resources and re-prioritisation given for the timely implementation of security patches; and re-enforcement by the IT Management Team, of the full ownership of this task by the technical team.

Ongoing user training is important in reducing the costs of end-user support. However this cost could be reduced, by exploiting the capabilities of the corporate Intranet system.

The need for a notification system and its ongoing maintenance could possibly be eliminated as a result of putting in place a sound process whereby system logs get reviewed every morning as a matter of priority.

Appendix A – References

CIS. "Windows 2000 Server Operating System Level 2 Benchmark": Consensus Baseline Security Settings (Stand-alone and Member Servers) URL: http://www.cisecurity.org/bench_win2000.html

"Top Ten Windows 2000 Security Practices webinar" URL: http://razor.bindview.com/publish/presentations/Top_Ten_Windows_2000.html

"Windows 2000 Security Checklist" URL: http://www.labmice.net/articles/securingwin2000.htm

"Windows 2000 Server Security Checklist" URL: http://windows.stanford,edu/docs/w2kservsecchecklist.htm

"Windows 2000 Server Baseline Security Checklist" URL: http://w2kinfo.nacs.uci.edu/Member_server_baseline_sec.htm

netiQ. "Securely Managing Your Group Policies". White Paper, 11 March 2002. URL: http://download.netiq.com/cms/NetIQ_WP_gpaSecurelyManagingGroupPolicies.pdf

Quest Software. "Advanced Security Management of Active Directory in Windows 2000". The White Papers, 15 May 2002 URL: http://www.quest.com/whitepapers/Quest-HP_AD_Security_WPFinal.pdf

Waddell, Johnny L. SANS. "Basic Security Issues of Active Directory". 11 June 2001. URL: http://www.sans.org/rr/win2000/active_dir.php

Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 1)". 2 December 2002. URL: http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_1.html

Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 2)". 20 December 2002. URL: http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_2.html

Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 3) – Backup and Restoration". 6 January 2003.
URL:
http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_3__Backup_and_Restoration.html

Magalhaes, Ricky M. "Securing Windows 2000 Active Directory (Part 4) - Restoration". 29 January 2003.
URL:
http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_4__Restoration.html

Microsoft. "Security Operations Guide for Windows 2000 Server". 2002.
Chapter 3 – Managing Security with Windows 2000 Group Policy
URL: http://www.microsoft.com/downloads/details.aspx?FamilyID=f0b7b4ee-201a-4b40-a0d2-cdd9775aeff8&DisplayLang=en (download link)

"Securing Windows 2000 Active Directory (Part 2)"
URL:
http://www.windowsecurity.com/articles/Securing_Windows_2000_Active_Directory_Part_2.html

Microsoft Knowledge Base Article - 289241
"A List of the Windows Server Domain Controller Default Ports"
URL: http://support.microsoft.com/default.aspx?scid=kb;en-us;Q289241

SANS. "Basic Security Issues of Active Directory"
URL: http://rr.sans.org

Microsoft. "Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations: Part I". Version 1.0
URL:
http://www.microsoft.com/downloads/details.aspx?displaylang=en&FamilyID=F937A913-F26E-49B5-A21E-20BA5930238D (download link)

SANS Posted Practicals for GIAC Systems and Network Auditor (GSNA) URL:
http://www.giac.org/cert.php

Tools Download Sources

@stake LC4 Password Auditing and Recovery Application
http://stake.com/research/lc/download.html

pwdump3 Windows NT/2000 remote password hash grabber
http://www.polivec.com/pwdumpdownload.html

SomarSoft Utilities
http://www.somarsoft.com/

Microsoft Baseline Security Analyzer
http://www.microsoft.com/technet/treeview/default.asp?url=/TechNet/Security/tools/tools/MBSAHome.ASP

Microsoft Windows 2000 SP3 Support Tools/Active Directory Support Tools
http://www.microsoft.com/windows2000/downloads/servicepacks/sp3/supporttools.ASP

Appendix B – Output File for SERVICES from the Somarsoft DumpSec Utility

26/04/2003 5:37 p.m. - Somarsoft DumpSec (formerly DumpAcl) - \\TestDC
FriendlyName   Name   Status   Type   Account

Alerter   Alerter   Running Win32   LocalSystem
Altiris Client Service   AClient   Running Win32   LocalSystem
Application Management   AppMgmt   Running Win32   LocalSystem
Automatic Updates   wuauserv   Running Win32   LocalSystem
Background Intelligent Transfer Service   BITS   Stopped Win32   LocalSystem
ClipBook   ClipSrv Stopped Win32   LocalSystem
COM+ Event System   EventSystem   Running Win32   LocalSystem
Compaq Event Notifier   CIMNotify   Stopped Win32   LocalSystem
Compaq Foundation Agents   CqMgHost   Running Win32   LocalSystem
Compaq NIC Agents   CPQNicMgmt   Running Win32   LocalSystem
Compaq Remote Monitor Service   CpqRcmc   Running Win32   LocalSystem
Compaq Server Agents   CqMgServ   Running Win32   LocalSystem
Compaq Storage Agents   CqMgStor   Running Win32   LocalSystem
Compaq Version Control Agent   cpqvcagent   Running Win32   LocalSystem
Compaq Web Agent   CpqWebMgmt   Running Win32   LocalSystem
Computer Browser   Browser Running Win32   LocalSystem
DefWatch   DefWatch   Running Win32   LocalSystem
DHCP Client   Dhcp   Running Win32   LocalSystem
DHCP Server   DHCPServer   Running Win32   LocalSystem
Distributed File System   Dfs   Running Win32   LocalSystem
Distributed Link Tracking Client   TrkWks Running Win32   LocalSystem
Distributed Link Tracking Server   TrkSvr   Running Win32   LocalSystem
Distributed Transaction Coordinator MSDTC Running Win32   LocalSystem
DNS Client   Dnscache   Running Win32   LocalSystem
DNS Server   DNS   Running Win32   LocalSystem
Event Log   Eventlog Running Win32   LocalSystem
Fax Service   Fax   Stopped Win32   LocalSystem
File Replication Service   NtFrs   Running Win32   LocalSystem
hp ProLiant System Shutdown Service   sysdown Running Win32   LocalSystem
IIS Admin ServiceIISADMIN   Running Win32   LocalSystem
Indexing Service   cisvc   Stopped Win32   LocalSystem
Intel Alert Handler   Intel Alert Handler   Running Win32   LocalSystem
Intel Alert Originator   Intel Alert Originator   Running Win32   LocalSystem
Intel File Transfer Intel File Transfer Running Win32   LocalSystem
Intel PDS   Intel PDS   Running Win32   LocalSystem
Internet Connection Sharing   SharedAccess   Stopped Win32   LocalSystem
Intersite Messaging   IsmServ Running Win32   LocalSystem
IPSEC Policy Agent   PolicyAgent   Running Win32   LocalSystem
Kerberos Key Distribution Center   kdc   Running Win32   LocalSystem
License Logging Service   LicenseService   Running Win32   LocalSystem
Logical Disk Manager   dmserver   Running Win32   LocalSystem
Logical Disk Manager Administrative Service dmadmin   Stopped Win32   LocalSystem
Messenger   Messenger   Running Win32   LocalSystem
Net Logon   Netlogon   Running Win32   LocalSystem
NetMeeting Remote Desktop Sharing   mnmsrvc   Stopped Win32   LocalSystem
Network Connections   Netman Running Win32   LocalSystem
Network DDE   NetDDE Stopped Win32   LocalSystem
Network DDE DSDM   NetDDEdsdm   Stopped Win32   LocalSystem
NT LM Security Support Provider   NtLmSsp   Running Win32   LocalSystem
Performance Logs and Alerts   SysmonLog   Stopped Win32   LocalSystem
Plug and Play   PlugPlayRunning Win32   LocalSystem
Print Spooler   Spooler Running Win32   LocalSystem
Protected Storage   ProtectedStorage Running Win32   LocalSystem
QoS RSVP   RSVP   Stopped Win32   LocalSystem

Remote Access Auto Connection Manager   RasAuto Stopped Win32   LocalSystem
Remote Access Connection Manager   RasMan Running Win32   LocalSystem
Remote Procedure Call (RPC)   RpcSs   Running Win32   LocalSystem
Remote Procedure Call (RPC) Locator   RpcLocator   Running Win32   LocalSystem
Remote Registry Service   RemoteRegistry Running Win32   LocalSystem
Removable Storage   NtmsSvc   Running Win32   LocalSystem
Routing and Remote Access   RemoteAccess   Stopped Win32   LocalSystem
RunAs Service   seclogon   Running Win32   LocalSystem
Security Accounts Manager   SamSs Running Win32   LocalSystem
Server   lanmanserver   Running Win32   LocalSystem
Smart Card   SCardSvr   Stopped Win32   LocalSystem
Smart Card Helper   SCardDrv   Stopped Win32   LocalSystem
SNMP Service   SNMP   Running Win32   LocalSystem
SNMP Trap Service   SNMPTRAP   Stopped Win32   LocalSystem
Surveyor   Surveyor   Running Win32   LocalSystem
Symantec AntiVirus ServerNorton AntiVirus Server   Running Win32   LocalSystem
System Event Notification   SENS   Running Win32   LocalSystem
Task Scheduler   Schedule   Running Win32   LocalSystem
TCP/IP NetBIOS Helper Service   LmHosts Running Win32   LocalSystem
Telephony   TapiSrv Running Win32   LocalSystem
Telnet   TlntSvr Stopped Win32   LocalSystem
Terminal Services   TermService   Running Win32   LocalSystem
Uninterruptible Power Supply   UPS   Stopped Win32   LocalSystem
Utility Manager   UtilMan Stopped Win32   LocalSystem
Windows Installer MSIServer   Stopped Win32   LocalSystem
Windows Internet Name Service (WINS)   WINS   Running Win32   LocalSystem
Windows Management Instrumentation   WinMgmt   Running Win32   LocalSystem
Windows Management Instrumentation Driver Extensions   Wmi   Running Win32   LocalSystem
Windows Time   W32Time   Running Win32   LocalSystem
Workstation   lanmanworkstation   Running Win32   LocalSystem
World Wide Web Publishing Service   W3SVC Running Win32   LocalSystem

Appendix C – DcDiag.Log (in non verbose mode)

Domain Controller Diagnosis

Performing initial setup:
   Done gathering initial info.

Doing initial required tests

   Testing server: TestDomain\TestDC1
      Starting test: Connectivity
         .... TestDC1 passed test Connectivity

Doing primary tests

   Testing server: TestDomain\TestDC1
      Starting test: Replications
         .... TestDC1 passed test Replications
      Starting test: NCSecDesc
         .... TestDC1 passed test NCSecDesc
      Starting test: NetLogons
         .... TestDC1 passed test NetLogons
      Starting test: Advertising
         .... TestDC1 passed test Advertising
      Starting test: KnowsOfRoleHolders
         .... TestDC1 passed test KnowsOfRoleHolders
      Starting test: RidManager
         .... TestDC1 passed test RidManager
      Starting test: MachineAccount
         .... TestDC1 passed test MachineAccount
      Starting test: Services
         .... TestDC1 passed test Services
      Starting test: ObjectsReplicated
         .... TestDC1 passed test ObjectsReplicated
      Starting test: frssysvol
         There are errors after the SYSVOL has been shared.
         The SYSVOL can prevent the AD from starting.
         .... TestDC1 passed test frssysvol
      Starting test: kccevent
         .... TestDC1 passed test kccevent
      Starting test: systemlog
         An Error Event occured. EventID: 0xC00010DF
            Time Generated: 04/26/2003   13:10:25
            Event String: A duplicate name has been detected on the TCP   An Error Event occured.
EventID: 0xC00010DF
            Time Generated: 04/26/2003   13:34:30
            Event String: A duplicate name has been detected on the TCP   .... TestDC1 failed
test systemlog

   Running enterprise tests on : XXXX.com
      Starting test: Intersite
         .... XXXX.com passed test Intersite
      Starting test: FsmoCheck
         .... XXXX.com passed test FsmoCheck

Appendix D – NetDiag.Log (in non verbose mode)

....

```
Computer Name: TestDC1
DNS Host Name: TestDC1.TestDomain1
System info : Windows 2000 Server (Build 2195)
Processor : x86 Family 6 Model 11 Stepping 1, GenuineIntel
List of installed hotfixes :
    Q147222
    q323172
    Q323255
    Q324096
    Q324380
    Q326830
    Q326886
    Q327696
    Q328145
    Q329115
    Q329834
```

Netcard queries test . . . . : Passed
    [WARNING] The net card 'Compaq NC3120 Fast Ethernet NIC' may not be working.

Per interface results:

    Adapter : Local Area Connection

        Netcard queries test . . . : Failed
        NetCard Status: DISCONNECTED
            Some tests will be skipped on this interface.

        Host Name. . . . . : TestDC1
        Autoconfiguration IP Address : x.x.x.x
        Subnet Mask. . . . . : x.x.x.x
        Default Gateway. . . . . . :
        Dns Servers. . . . . :

    Adapter : Team

        Netcard queries test . . . : Passed

        Host Name. . . . . : TestDC1
        IP Address . . . . : x.x.x.x
        Subnet Mask. . . . . : x.x.x.x
        Default Gateway. . . . . . : x.x.x.x
        Dns Servers. . . . . : x.x.x.x
                                     x.x.x.x

        AutoConfiguration results. . . . . . : Passed

        Default gateway test . . . : Passed

        NetBT name test. . . . . . : Passed

        WINS service test. . . . . : Skipped
            There are no WINS servers configured for this interface.

Global results:

Domain membership test . . . . . . : Passed

NetBT transports test. . . . . . . : Passed
    List of NetBt transports currently configured:
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
    2 NetBt transports currently configured.

Autonet address test . . . . : Passed

IP loopback ping test. . . . . . . : Passed

Default gateway test . . . . : Passed

NetBT name test. . . . . : Passed

Winsock test . . . . : Passed

DNS test . . . . : Failed
    [WARNING] The DNS entries for this DC are not registered correctly on DNS server 'x.x.x.x'. Please wait
for 30 minutes for DNS server replication.
    [WARNING] The DNS entries for this DC are not registered correctly on DNS server 'x.x.x.x'. Please wait
for 30 minutes for DNS server replication.
    [FATAL] No DNS servers have the DNS records for this DC registered.

Redir and Browser test . . . . . . : Passed
    List of NetBt transports currently bound to the Redir
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
    The redir is bound to 2 NetBt transports.

    List of NetBt transports currently bound to the browser
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
        NetBT_Tcpip_{xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx}
    The browser is bound to 2 NetBt transports.

DC discovery test. . . . . : Passed

DC list test . . . . : Passed

Trust relationship test. . . . . . : Skipped

Kerberos test. . . . . : Passed

LDAP test. . . . . : Passed

Bindings test. . . . . : Passed

WAN configuration test . . . . . . : Skipped
    No active remote access connections.

Modem diagnostics test . . . . . . : Passed

IP Security test . . . . : Passed
    IPSec policy service is active, but no policy is assigned.

The command completed successfully

Appendix E – Specific References from Microsoft. Best Practice Guide for Securing Active Directory Installations and Day-to-Day Operations:Part I

Table 9   Recommended Services to Install on a Windows 2000 Server

Service Name	Default Startup Type	Recommended Startup Type	Comment
Alerter	Automatic	(No change)	Notifies selected users and computers of administrative alerts.
Application Management	Manual	(See comment)	Provides software installation services for applications that are deployed through Add/Remote Programs. On dedicated domain controllers, this service can be disabled to prevent unauthorized installation of software.
Automatic Updates	Automatic	(See comment)	Provides the download and installation of critical Windows updates, such as security patches or hotfixes. This service an be disabled when automatic updates are not performed on the domain controller. It is included when SP3 is applied.
Background Intelligent Transfer Service	Manual	(See comment)	Provides a background file transfer mechanism and queue management, and it is used by Automatic Update to automatically download programs (such as security patches). This service can be disabled when automatic updates are not performed on the domain controller. It is included when SP3 is applied.
ClipBook	Manual	(See comment)	Enables the Clipbook Viewer to create and share "pages" of data to be reviewed by remote users. On dedicated domain controllers, this service can be disabled.
COM+ Event System	Manual	(No change)	Provides automatic distribution of events to COM components.
Computer Browser	Automatic	(No change)	Maintains the list of computers on the network, and supplies the list to programs that request the list.

Service Name	Default Startup Type	Recommended Startup Type	Comment
DHCP Client	Automatic	(No change)	Required to update records in Dynamic DNS.
Distributed File System	Automatic	(No change)	Manages logical volumes that are distributed across a local area network (LAN) or wide area network (WAN), and it is required for the Active Directory SYSVOL share.
Distributed Link Tracking Client	Automatic	Disabled	Maintains links between NTFS v5 file system files within the domain controllers and other servers in the domain. Disable Distributed Link Tracking Client on dedicated domain controllers.
Distributed Link Tracking Server	Manual	Disabled	Tracks information about files that are moved between NTFS v5 volumes throughout a domain. Disable Distributed Link Tracking Server on dedicated domain controllers.
DNS Client	Automatic	(No change)	Allows resolution of DNS names.
DNS Server	Automatic	(No change)	Required for Active Directory–integrated DNS zones.
Event Log	Automatic	(No change)	Writes event log messages that are issued by Windows-based programs and components to the log files.
Fax Service	Manual	Disabled	Provides the ability to send and receive faxes through fax resources that are available on the domain controller and network. On dedicated domain controllers, this service can be disabled because sending and receiving faxes is not a normal function of a domain controller.
File Replication Service	Manual	(No change)	Enables files to be automatically copied and maintained simultaneously on multiple computers, and it is used to replicate SYSVOL among all domain controllers.
Indexing Service	Manual	(See comment)	Indexes content and properties of files on the domain controller to provide rapid access to the file through a flexible querying language. On dedicated domain controllers, disable this service to prevent users from searching files and file content if sensitive files and folders are inadvertently indexed.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Internet Connection Sharing	Manual	Disabled	Provides network address translation (NAT), addressing and name resolution, and intrusion detection when connected through a dial-up or broadband connection. On dedicated domain controllers, disable to prevent inadvertent enabling of NAT, which would prevent the domain controller from communicating with the remainder of the network.
Intersite Messaging	Disabled	(No changes)	Required by SMTP replication in Active Directory, DFS, and NETLOGON.
IPSEC Policy Agent	Automatic	(No change)	Provides management and coordination of Internet Protocol Security (IPSec) policies with the IPSec driver.
Kerberos Key Distribution enter	Disabled	(No change)	Provides the ability for users to log on using the Kerberos V5 authentication protocol.
License Logging Service	Automatic	(See comment)	Monitors and records client access licensing for portions of the operating system, such as IIS, Terminal Services, and file and print sharing, and for products that are not a part of the operating system, such as Microsoft SQL Server or Microsoft Exchange Server. On a dedicated domain controller, this service can be disabled.
Logical Disk Manager	Automatic	(No change)	Required to ensure that dynamic disk information is up to date.
Logical Disk Manager Administrative Service	Manual	(No change)	Required to perform disk administration.
Messenger	Automatic	(No change)	Transmits net sends and Alerter service messages between clients and servers.
Net Logon	Manual	(No change)	Maintains a secure channel between the domain controller, other domain controllers, member servers, and workstations in the same domain and trusting domains.
NetMeeting Remote Desktop Sharing	Manual	Disabled	Eliminates potential security threat by allowing domain controller remote administration through NetMeeting.
Network Connections	Manual	(No change)	Manages objects in the Network Connections folder.
Network DDE	Manual	(See comment)	Provides network transport and security for Dynamic Data Exchange (DDE) for programs running on the domain controller. This service can be disabled when no DDE applications are running locally on the domain controller.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Network DDE DSDM	Manual	(See comment)	Used by Network DDE. This service can be disabled when Network DDE is disabled.
NTLM Security Support Provider	Manual	(No change)	Provides security to RPC programs that use transports other than named pipes, and enables users to log on using the NTLM authentication protocol.
Performance Logs and Alerts	Manual	(See comment)	Collects performance data for the domain controller, writes the data to a log, or generates alerts. This service can be set to automatic when you want to log performance data or generate alerts without an administrator being logged on.
Plug and Play	Automatic	(No change)	Required to automatically recognize and adapt to changes in the domain controller hardware with little or no user input.
Print Spooler	Automatic	(See comment)	Manages all local and network print queues and controls all print jobs. Can be disabled on dedicated domain controllers where no printing is required.
Protected Storage	Automatic	(No change)	Protects storage of sensitive information, such as private keys, and prevents access by unauthorized services, processes, or users. This service is used on domain controllers for smart card logon.
QoS RSVP	Manual	(See comment)	Provides support for QoS RSVP routing information. This service an be disabled when QoS is not used to allocate network bandwidth in network infrastructure.
Remote Access Auto Connection Manager	Manual	(See comment)	Detects unsuccessful attempts to connect to a remote network or computer and provides alternative methods for connection. This service can be disabled on dedicated domain controllers where no virtual private network (VPN) or dial-up connections are initiated.
Remote Access Connection Manager	Manual	(See comment)	Manages VPN and dial-up connection from the domain controller to the Internet or other remote networks. This service can be disabled on dedicated domain controllers where no VPN or dial-up connections are initiated.
Remote Procedure Call (RPC)	Manual	(No change)	Serves as the RPC endpoint mapper for all applications and services that use RPC communications.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Remote Procedure Call (RPC) Locater	Automatic	(See comment)	Enables RPC clients using the RpcNs* family of application programming interfaces (APIs) to locate RPC servers and manage the RPC name service database. This service can be disabled if no applications use the RpcNs* APIs.
Remote Registry Service	Automatic	(No change)	Enables remote users to modify registry settings on the domain controller, provided the remote users have the required permissions. By default, only Administrators and Backup Operators can access the registry remotely.
Removable Storage	Automatic	(See comment)	Manages and catalogs removable media, and operates automated removable media devices, such as tape auto loaders or CD jukeboxes. This service can be disabled when removable media devices are directly connected to the domain controller.
Routing and Remote Access	Disabled	(No change)	Enables LAN-to-LAN, LAN-to-WAN, VPN, and NAT routing services.
RunAs Service	Automatic	(No change)	Allows you to run specific tools and programs with different privileges than your current logon provides.
Security Accounts Manager	Automatic	(No change)	A protected subsystem that manages user and group account information.
Server	Automatic	(No change)	Provides RPC support, file print, and named pipe sharing over the network.
Smart Card	Manual	(No change)	Manages and controls access to a smart card that is inserted into a smart card reader attached to the domain controller.
Smart Card Helper	Manual	(No change)	Provides support for legacy, non-plug-and-play smart card readers.
System Event Notification	Automatic	(No change)	Monitors system events and notifies subscribers to the COM+ Event System of these events.
Task Scheduler	Automatic	(No change)	Provides the ability to schedule automated tasks on the domain controller.
TCP/IP NetBIOS Helper Service	Automatic	(No change)	Provides support for the NetBIOS over TCP/IP (NetBT) service and NetBIOS name resolution for clients.

Service Name	Default Startup Type	Recommended Startup Type	Comment
Telephony	Manual	(See comment)	Provides Telephony API (TAPI) support of client programs that control telephony devices and IP-based voice connections. This service can be disabled on dedicated domain controllers where TAPI is not used by applications.
Telnet	Manual	Disabled	Enables a remote user to log on and run applications from a command line on the domain controller. Enable Telnet only when it is used for remote administration for branch offices or headless domain controllers. Terminal Services is the recommended method for remote administration.
Terminal Services	Disabled	(See comment)	Allows multiple remote users to be connected interactively to the domain controller, and provides display of desktops and run applications. To reduce the surface area of attack, disable Terminal Services unless it is used for remote administration for branch offices or headless domain controllers.
Uninterruptible Power Supply	Automatic	(No change)	Manages an uninterruptible power supply (UPS) that is connected to the domain controller by a serial port.
Utility Manager	Manual	Disabled	Allows faster access to some accessibility tools, such as Magnifier, Narrator, and On-Screen Keyboard, and also displays the status of the tools or devices that it controls. Disable Utility Manager unless you require these special accessibility tools.
Windows Installer	Manual	(No change)	Adds, modifies, and removes applications that are provided as a Windows Installer (.MSI) package.
Windows Management Instrumentation	Manual	(No change)	Provides a common interface and object model to access management information about the domain controller through the WMI interface.
Windows Management Instrumentation Drivers	Manual	(No change)	Monitors all drivers and event trace providers that are configured to publish WMI or event trace information.
Windows Time	Manual	(No change)	Sets the domain controller clock, and maintains date and time synchronization on all computers in the network.
Workstation	Automatic	(No change)	Creates and maintains client network connections to remote servers.

Table 11   Additional Files and Folders to Be Secured After Promotion to Domain Controller

File or Folder	Permissions
Root of each logical disk volume	• Allow Read and Execute for Everyone. • Allow Full Control for Administrators.

Table 12   Default and Recommended Password Group Policy Settings

Policy	Default	Recommended	Comments
Enforce password history	1 passwords	24 passwords	Prevents users from reusing passwords.
Maximum password age	42 days	(No change)	
Minimum password age	0 days	2 days	Prevents users from cycling through their password history to reuse passwords.
Minimum password length	0 characters	8 characters	Ensures minimum password strength.
Password must meet complexity requirements	Disabled	Enable	For the definition of a complex password, see "Creating a Strong Administrator Password" in this chapter.
Store password using reverse encryption for all users in domain	Disabled	(No change)	

Table 13   Default and Recommended Account Lockout Group Policy Settings

Policy	Default	Recommended	Reason
Account lockout duration	Not defined	0 minutes	The value 0 means that after account lockout an Administrator is required to re-enable the account before account lockout reset has expired.
Account lockout threshold	0 tries	5 tries	The value 0 means that failed password tries never cause account lockout.
Reset account lockout counter after	Not defined	30 minutes	This setting protects against a sustained dictionary attack by imposing a nontrivial delay after 5 unsuccessful attempts. A higher value for this setting could result in increased help-desk calls for legitimate account lockouts.

Table 14 Default and Recommended Kerberos Group Policy Settings

Policy	Default	Recommended	Comments
Enforce user logon restrictions	Enabled	(No change)	A user must have the right to log on locally (for service on the same computer) or to access the service from the network.
Maximum lifetime for service ticket	600 minutes	(No change)	
Maximum lifetime for user ticket	10 hours	(No change)	
Maximum lifetime for user ticket renewal	7 days	(No change)	
Maximum tolerance for computer clock synchronization	5 minutes	(No change)	Maximum tolerance between the client's and server's clocks.

Table 15 Default and Recommended Domain Controller User Rights Assignment Policy Settings

Policy	Default Setting	Recommended Setting	Comments
Log on locally	Administrators Backup Operators Account Operators Server Operators	Administrators Backup Operators Server Operators	Account Operators are for account management and have few (if any) reasons to log on locally.
Shut down the system	Administrators Backup Operators Account Operators Server Operators Print Operators	Administrators Backup Operators Server Operators	Account Operators and Print Operators have few (if any) reasons to shut down domain controllers.

Table 16 Default and Recommended Domain Controller Audit Policy Settings

Policy	Default Setting	Recommended Setting	Comments
Audit account logon events	No auditing	Success	Account logon events are generated when a domain user account is authenticated on a domain controller.
Audit account management	Not defined	Success	Account management events are generated when security principal accounts are created, modified, or deleted.
Audit directory service access	No auditing	Success	Directory services access events are generated when an Active Directory object with a system access control list (SACL) is accessed.

Policy	Default Setting	Recommended Setting	Comments
Audit logon events	No auditing	Success	Logon events are generated when a domain user interactively logs on to a domain controller or a network logon to a domain controller is performed to retrieve logon scripts and policies.

Table 29   Recommended Domain Controller Security Options Policy Settings

Policy	Default Setting	Recommended Setting	Comments
Additional restrictions for anonymous connections	Not defined	(See comments)	For operating system requirements, see "Selecting Policy Settings for Mixed Operating System Environments."
Allow Server Operators to schedule tasks (domain controllers only)	Not defined	Disabled	Restricts the individuals who can schedule tasks to Administrators, because scheduling usually runs as an elevated service.
Allow system to be shut down without having to log on	Not defined	Disabled	Requires an authenticated, authorized service account to shut down or restart the domain controller.
Allow to eject removable NTFS media	Not defined	Administrators	Allows only Administrators to eject removable NTFS media to protect against the theft of sensitive data.
Amount of idle time required before disconnecting session	Not defined	15 minutes	Controls when a domain controller suspends an inactive server message block (SMB) session, which has no security implications but which reduces SMB traffic resource usage.
Audit the access of global system objects	Not defined	Disabled	Disables the creation of a default SACL on system objects, such as mutexes(mutual exclusive), events, semaphores, and DOS devices because the default policy is "No auditing."
Audit use of Backup and Restore privilege	Not defined	Disabled	Disables auditing for the use of user privileges, including Backup and Restore, when the "Audit privilege use" policy is enabled because this policy is configured for "No auditing."
Automatically log off users when logon time expires	Not defined	Enabled	Forcibly disconnects client sessions with the SMB Service when the user's logon hours expire to ensure that network connections are secured during nonworking hours.

Policy	Default Setting	Recommended Setting	Comments
Automatically log off users when logon time expires (local)	Not defined	Enabled	Forcibly logs off users with interactive sessions when the user's logon hours expire to ensure that network connections are secured during nonworking hours.
Clear virtual memory pagefile when system shuts down	Not defined	Enabled	Eliminates process memory data from going into the pagefile on shutdown in case an unauthorized user manages to directly access the pagefile.
Digitally sign client communication (always)	Not defined	(See comments)	See "Selecting Policy Settings for Mixed Operating System Environments" for requirements.
Digitally sign client communication (when possible)	Not defined	(No change)	See "Selecting Policy Settings for Mixed Operating System Environments" for requirements.
Digitally sign server communication (always)	Not defined	(See comments)	See "Selecting Policy Settings for Mixed Operating System Environments" for requirements.
Digitally sign server communication (when possible)	Enabled	(No change)	See "Selecting Policy Settings for Mixed Operating System Environments" for requirements.
Disable CTRL + ALT + DEL requirement for logon	Not defined	Disabled	Requires CTRL+ALT+DEL before users log on to ensure that users are communicating by means of a trusted path when entering their passwords.
Do not display last user name in logon screen	Not defined	Enabled	Removes the name of the last user to successfully log off from the **Log On to Windows** dialog box to prevent attackers from discovering service account names on domain controllers.
LAN Manager Authentication Level	Not defined	(See comments)	See "Selecting Policy Settings for Mixed Operating System Environments" for requirements.
Message text for users attempting to log on	Not defined	(No change)	
Message title for users attempting to log on	Not defined	(No change)	
Number of previous logons to cache (in case domain controller is not available)	Not defined	0 logons	The value 0 indicates that the domain controller does not cache previous logons and requires authentication at each logon.

Policy	Default Setting	Recommended Setting	Comments
Prevent system maintenance of computer account password	Not defined	Disabled	Not enabled because computer account passwords are used to establish secure channel communications between members and domain controllers and, within the domain, between the domain controllers themselves. After it is established, the secure channel is used to transmit sensitive information that is necessary for making authentication and authorization decisions.
Prevent users from installing printer drivers	Not defined	Enabled	Allows only Administrators and Server Operators to install a printer driver when adding a network printer to ensure that users cannot install a printer driver (add a network printer) and perform disk-space attacks by submitting large print jobs.
Prompt user to change password before expiration	Not defined	14 days	Notifies users in advance (in days) that their password is about to expire so that the user has time to construct a password that is sufficiently strong.
Recovery Console: Allow automatic administrative logon	Not defined	Disabled	Requires that an Administrator account password must be given before access is granted to a domain controller to ensure that anyone logging on requires administrator credentials.
Recovery Console: Allow floppy copy and access to all drivers and all folders	Not defined	Disabled	Prevents unauthorized users from gaining access to, copying, and removing the Active Directory database and other secure files from the domain controller.
Rename administrator account	Not defined	(No change)	
Rename guest account	Not defined	(No change)	
Restrict CD-ROM access to locally logged-on users only	Not defined	Enabled	Allows only the interactively logged-on service administrator to access removable CD-ROM media to ensure that when no one is logged on interactively, the CD-ROM cannot be accessed over the network.
Restrict floppy access to locally logged-on users only	Not defined	Enabled	Allows only interactively logged-on service administrators to access removable floppy media to ensure that the floppy cannot be accessed over the network when no one is logged on.

Policy	Default Setting	Recommended Setting	Comments
Secure channel: Digitally encrypt or sign secure channel data (always)	Not defined	Enabled	Requires Windows NT 4.0 with Service Pack 6 or newer software on all domain controllers in local and all trusted domains to ensure that all security fixes have been made.
Secure channel: Digitally encrypt secure channel data (when possible)	Not defined	(No change)	
Secure channel: Digitally sign secure channel data (when possible)	Not defined	(No change)	
Secure channel: Require strong (Windows 2000 or later) session key	Not defined	Enabled	Requires that a secure channel be established with 128-bit encryption to ensure that the key strength is not negotiated but always uses the most secure connection possible with the domain controller.
Secure system partition (for RISC platforms only)	Not defined	(No change)	
Send unencrypted password to connect to third-party SMB servers	Not defined	Disabled	Prohibits the SMB redirector from sending plaintext passwords to non-Microsoft SMB servers that do not support password encryption. Disable this policy unless your domain controller needs to communicate with non-Microsoft SMB servers.
Shut down system immediately if unable to log security audits	Not defined	Disabled	Stops the domain controller if a security audit cannot be logged. The auditing goals for domain controllers, in "Establishing Domain Controller Audit Policy Settings" allow overwriting Security audit events as required.
Smart card removal behavior	Not defined	Force logoff	Forces service administrators to keep smart cards inserted while logged on interactively on domain controllers to ensure that domain controllers are not left logged on to and unattended.
Strengthen default permissions of global system objects (e.g. Symbolic Links)	Not defined	Enabled	Allows users who are not administrators to read shared objects but not modify them. Strengthens the default DACL of objects in the global list of shared resources, such as DOS device names, mutexes, and semaphores.
Unsigned driver installation behavior	Not defined	Do not allow installation	Prevents insecure or untrusted device drivers from being installed on domain controllers.

Policy	Default Setting	Recommended Setting	Comments
Unsigned non-driver installation behavior	Not defined	Silently succeed	Nondriver signing was not implemented in most software applications and services. Policy has no real benefit and is set to eliminate unnecessary notification.

Table 30   Recommended Domain Controller Event Log Policy Settings

Policy	Default Setting	Recommended Setting	Comments
Maximum application log size	Not defined	(No change)	
Maximum security log size	Not defined	128 MB	Increased to accommodate security auditing that is enabled in the domain controller audit policies.
Maximum system log size	Not defined	(No change)	
Prevent local guests group from accessing application log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the application log events.
Prevent local guests group from accessing security log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the security log events.
Prevent local guests group from accessing system log	Not defined	Enabled	Prevents members of the built-in group Guests from reading the system log events.
Retain application log	Not defined	(No change)	
Retain security log	Not defined	(No change)	
Retain system log	Not defined	(No change)	
Retention method for application log	Not defined	(No change)	
Retention method for security log	Not defined	Overwrite events as needed	Overwrites the security log when the maximum log size is reached to ensure that the log contains the most recent security events and to ensure that logging continues.
Retention method for system log	Not defined	Overwrite events as needed	Overwrites the system log when the maximum log size is reached to ensure that the log contains the most recent security events and to ensure that logging continues.
Shutdown the computer when the security audit log is full	Not defined	(No change)	