

[a] Boot Sequence—System Bootup

System Bootup

Yes No

Bios has password
System boots to IDE-0 first

Exceptions:

[b] Physical Security

Yes No

Server prompts for password
Server can be locked with CTRL + ALT + DELETE
Server has screensaver
Screen Saver is activated in 15 minutes or less

Exceptions:

[c] Software Version

Microsoft Windows _____
Version 5.0, Build: _____
Service Pack: _____
Licensed to: _____
Server Name: _____
Company Name: _____

Exceptions:

[d] Software License

Yes No

Obtained from original media
License Key:

Exceptions:

[e] Time Is Properly Set

Yes No

Manually:
Agent:
Active Directory:

Exceptions:

[f] Network Configuration

Yes No

Server uses TCP/IP only

Fixed IP Address only

IP Address is:

Workgroup only

Exceptions:

[g] Drives Are Properly Formatted

Drive Partitions: _____

Yes No

NTFS Partitions only

Exceptions:

[h] Drives Are Properly Partitioned

Yes No

System and Data files on separate partitions

System Directories renamed

System Directory name _____

Exceptions:

[i] NTFS Disk Permissions

Yes No

“Everyone” has been removed

Name:

Permissions:

Administrator

Authenticated Users

Creator/Owner

System

Yes No

Default Share Permissions have been removed

Hidden Share Permissions have been removed

Exceptions:

[j] Directory Permissions

Yes No

Directory Shares have been removed
Critical Directory Permission Granted only to
Administrators, CREATOR OWNER and System

Critical Directory Names: _____

Exceptions:

[k] File Permissions

Yes No

“Everyone” has been removed

Name:	Permissions:
Administrator	
Authenticated Users	
Creator/Owner	

Yes No

Inheritance is turned on
System file access is restricted
Registry Access is restricted
Executables are restricted

Exceptions:

[l] Unnecessary Accounts Are Removed or Disabled

Yes No

Administrator Account has been renamed
Systems Administrators use individual Accounts
Guest Account has been removed
TsInternetUser is disabled

Exceptions:

[m] Anonymous Access Is Restricted

Yes No

Anonymous Access Restricted

Exceptions:

[n] Unnecessary Protocols Are Disabled

Yes No

Unnecessary protocols disabled

Exceptions:

[o] Unnecessary Subsystems Are Removed

Yes No

Subsystems removed

Exceptions:

[p] Unnecessary Services Are Removed

Yes No

Unnecessary services removed

Exceptions:

[q] Unnecessary Programs Are Removed

Yes No

Unnecessary programs removed

Exceptions:

Dangerous Programs Are Secured

Yes No

Dangerous programs are secured

Exceptions:

[r] Current Service Packs Are Installed

Yes No

Current Services Packs
Current Hotfixes
Manual or Automatic Update process in place

Exceptions:

[s] **Auditing Is Enabled**

Server is auditing and logging:

Policy	Yes	No
Account Log-on Events		
Account Management		
Directory Access		
Log-on Events		
Object Access		
Policy Change		
Privilege Use		
Process Tracking		
System Events		

Audit Log size:

Audit Logs "Overwrite Events as Needed"

How often are Audit Logs are reviewed?

Policy **Who can perform? (Circle)**

Access this computer from the network:

Administrators, Backup Operators, Power Users, Users, Guest

Act as part of the operating system:

Administrators, Backup Operators, Power Users, Users, Guest

Add workstations to domain:

Administrators, Backup Operators, Power Users, Users, Guest

Back up files and directories:

Administrators, Backup Operators, Power Users, Users, Guest

Bypass traverse checking:

Administrators, Backup Operators, Power Users, Users, Guest

Change the system time:

Administrators, Backup Operators, Power Users, Users, Guest

Create a pagefile:

Administrators, Backup Operators, Power Users, Users, Guest

Create a token object:

Administrators, Backup Operators, Power Users, Users, Guest

Create permanent shared objects:

Administrators, Backup Operators, Power Users, Users, Guest

Debug programs:

Administrators, Backup Operators, Power Users, Users, Guest

Deny access to this computer from the network:

Administrators, Backup Operators, Power Users, Users, Guest

Deny log-on as a batch job:

Administrators, Backup Operators, Power Users, Users, Guest

Deny log-on as a service:

Administrators, Backup Operators, Power Users, Users, Guest

Deny log-on locally:

Administrators, Backup Operators, Power Users, Users, Guest

Enable computer and user accounts to be trusted for delegation:

Administrators, Backup Operators, Power Users, Users, Guest

Force shutdown from a remote system:

Administrators, Backup Operators, Power Users, Users, Guest

Generate security audits:

Administrators, Backup Operators, Power Users, Users, Guest

Increase quotas:

Administrators, Backup Operators, Power Users, Users, Guest

Increase scheduling priority:

Administrators, Backup Operators, Power Users, Users, Guest

Load and unload device drivers:

Administrators, Backup Operators, Power Users, Users, Guest

Lock pages in memory:

Administrators, Backup Operators, Power Users, Users, Guest

Log on as a batch job:

Administrators, Backup Operators, Power Users, Users, Guest

Log on as a service:

Administrators, Backup Operators, Power Users, Users, Guest

Log on locally:

Administrators, Backup Operators, Power Users, Users, Guest

Manage auditing and security log:

Administrators, Backup Operators, Power Users, Users, Guest

Modify firmware environment values:

Administrators, Backup Operators, Power Users, Users, Guest

Profile single process:

Administrators, Backup Operators, Power Users, Users, Guest

Profile system performance:

Administrators, Backup Operators, Power Users, Users, Guest

Replace a process level token:

Administrators, Backup Operators, Power Users, Users, Guest

Restore files and directories:

Administrators, Backup Operators, Power Users, Users, Guest

Shut down the system:

Administrators, Backup Operators, Power Users, Users, Guest

Synchronize directory service data:

Administrators, Backup Operators, Power Users, Users, Guest

Take ownership of files or other objects:

Administrators, Backup Operators, Power Users, Users, Guest

Exceptions:

[t] **Security Settings**

Password Policies

Policy	Setting	Description
Password history enforced		
Maximum password age		
Minimum password age		
Minimum password length		
Passwords meet complexity requirements		

Exceptions:

Account Lockout Policies

Policy	Setting	Description
Account Lockout Duration		
Number of Attempts		

Account Reset in Minutes

Exceptions:

User Rights

Exceptions:

Security Options

Security options are set.

Selected Settings:

Policy	Setting (Circle)	
Additional restrictions for anonymous connections	Y	N
Allow system to be shut down without having to log on	E	D
Allowed to eject removable NTFS media	E	D
Amount of idle time required before disconnecting session	__	mins.
Audit use of Backup and Restore privilege	E	D
Automatically log off users when log-on time expires (local)	E	D
Clear virtual memory pagefile when system shuts down	E	D
Disable CTRL+ALT+DEL requirement for log-on	E	D
Do not display last user name in log-on screen	E	D
Message text for users attempting to log on	Y	N
Message title for users attempting to log on	Y	N
Prompt user to change password before expiration	__	days
Recovery Console: Allow automatic administrative log-on	E	D
Recovery Console: Allow floppy copy and access to all drives and all folders	E	D
Rename administrator account	E	D
Rename guest account	E	D
Restrict CD-ROM access to locally logged-on user only	E	D
Restrict floppy access to locally logged-on user only	E	D
Secure channel: Digitally encrypt or sign secure channel data (always)	E	D
Secure channel: Digitally encrypt secure channel data (when possible)	E	D
Secure channel: Digitally sign secure channel data (when possible)	E	D
Secure channel: Require strong (Windows 2000 or later) session key	E	D
Send unencrypted password to connect to third-party SMB servers	E	D
Shut down system immediately if unable to log security audits	E	D

Strengthen default permissions of global system objects	E	D
Unsigned driver installation behavior	E	D
Unsigned non-driver installation behavior	E	D

Exceptions:

Public Key Policy

Public Key Policy	Y	N
-------------------	---	---

Exceptions:

IP Security Policies on Local Machine

IP Security Policies	Y	N
----------------------	---	---

Exceptions:

[u] Antivirus Software and Updates Have Been Installed

Antivirus Software: _____
 Current Revision: _____
 Last Update: _____
 Update Method: _____

Exceptions:

[v] System and Security Are Documented

Document Created: _____
 Document Updates: _____

Exceptions:

[w] Staff Training

Staff Certifications: _____
 Experience Levels: _____
 Windows 2000 Specific: _____

Recommendations: