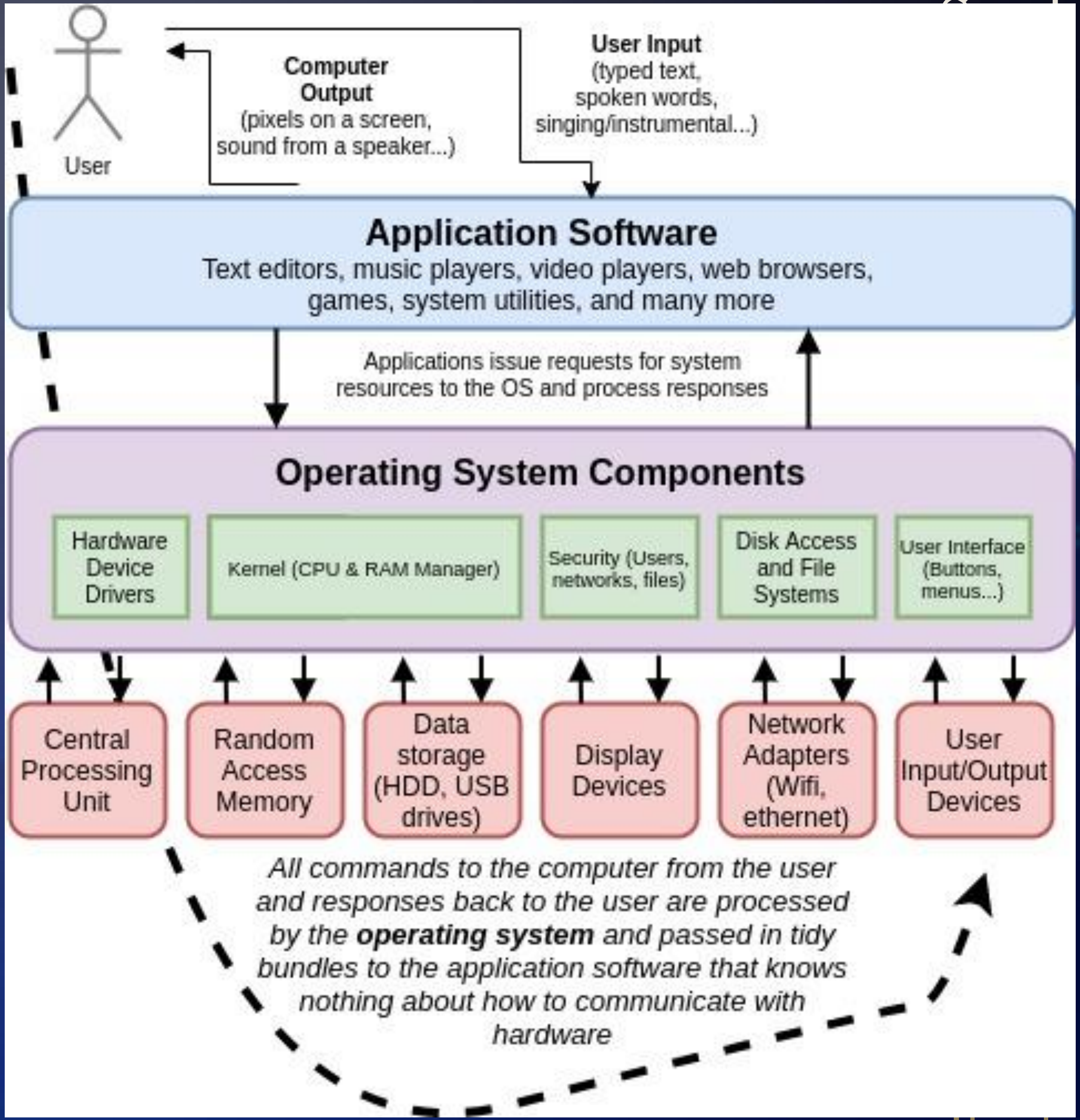
MODULE 4A: AUDITING WINDOWS DEVICES

OBJECTIVES

- Windows essentials: learning about the target host
- How to audit Windows servers
- Tools and resources for enhancing your Windows audits

WHAT IS THE OPERATING SYSTEM?

- Operating System is typically the interface between applications, and the hardware & networking equipment that processes and transfers that data internally within the system, and outside of the system, respectively.



User

Computer Output
(pixels on a screen, sound from a speaker...)

User Input
(typed text, spoken words, singing/instrumental...)

Application Software
Text editors, music players, video players, web browsers, games, system utilities, and many more

Applications issue requests for system resources to the OS and process responses

Operating System Components

Hardware Device Drivers

Kernel (CPU & RAM Manager)

Security (Users, networks, files)

Disk Access and File Systems

User Interface (Buttons, menus...)

Central Processing Unit

Random Access Memory

Data storage (HDD, USB drives)

Display Devices

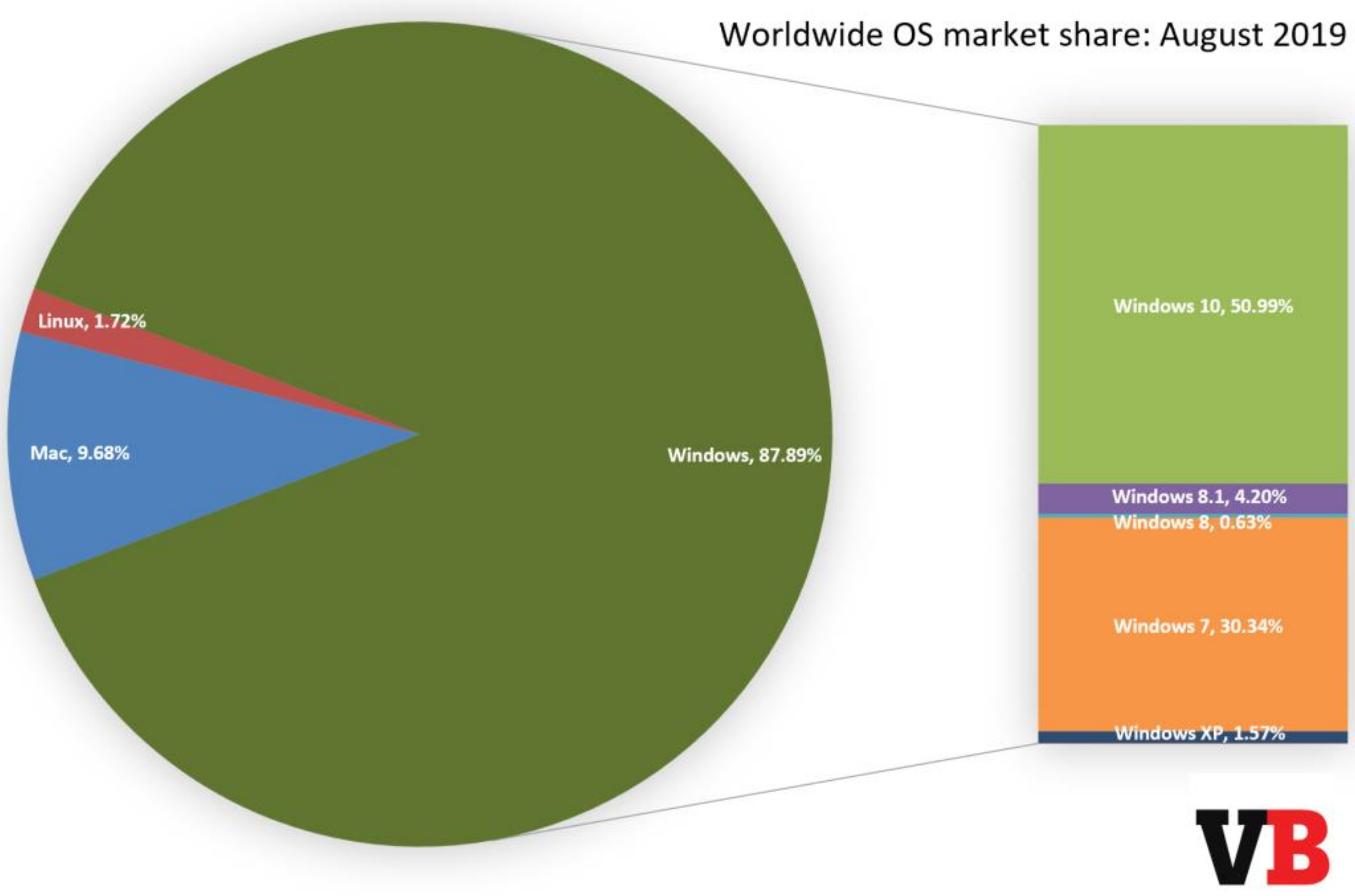
Network Adapters (Wifi, ethernet)

User Input/Output Devices

*All commands to the computer from the user and responses back to the user are processed by the **operating system** and passed in tidy bundles to the application software that knows nothing about how to communicate with hardware*

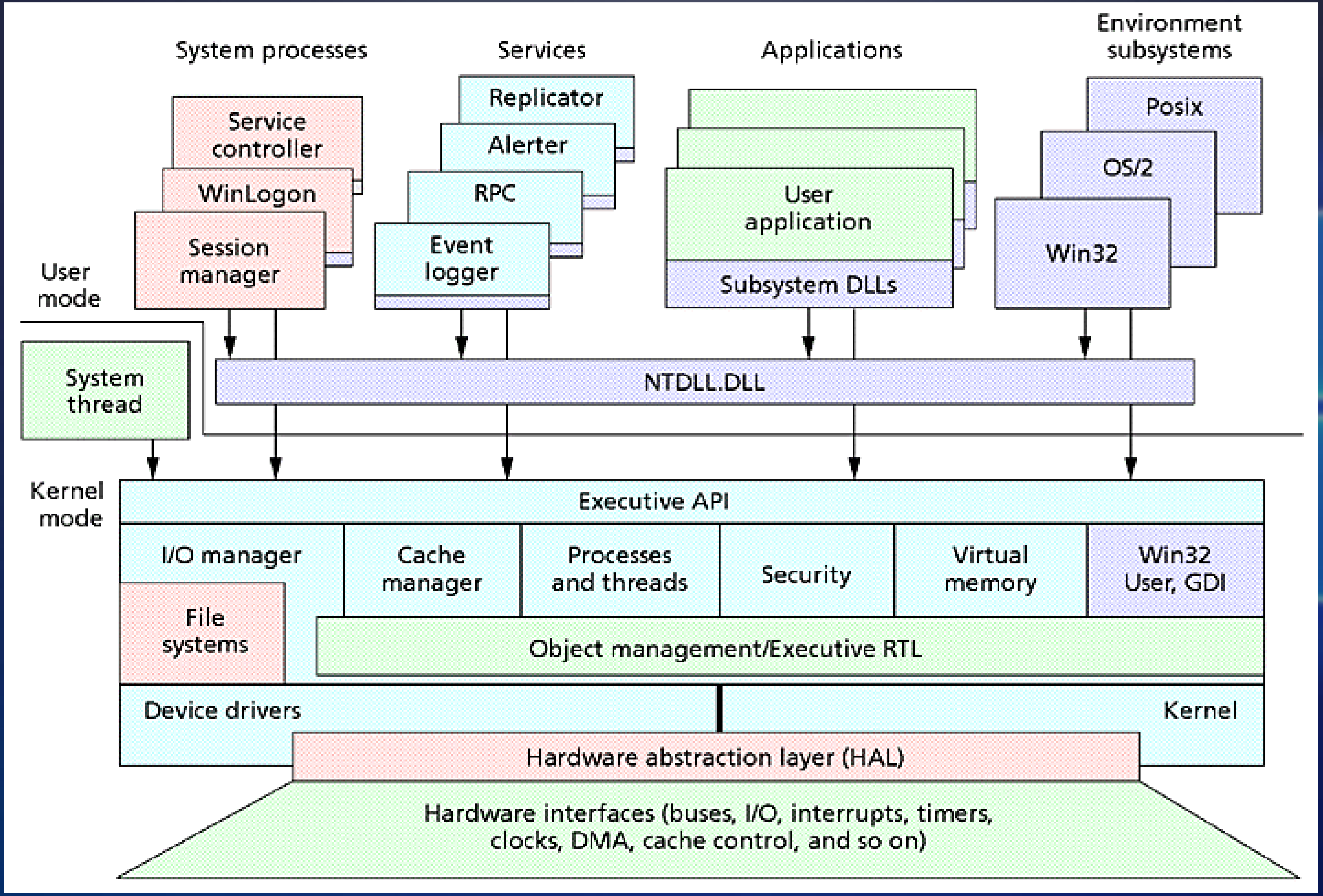
https://technologyrediscovery.net/compFund/obcat.comp.os.html

WINDOWS AND DESKTOP OS DOMINANCE



https://venturebeat.com/2019/09/01/net-applications-windows-10-windows-7-market-share/

WINDOWS NT ARCHITECTURE



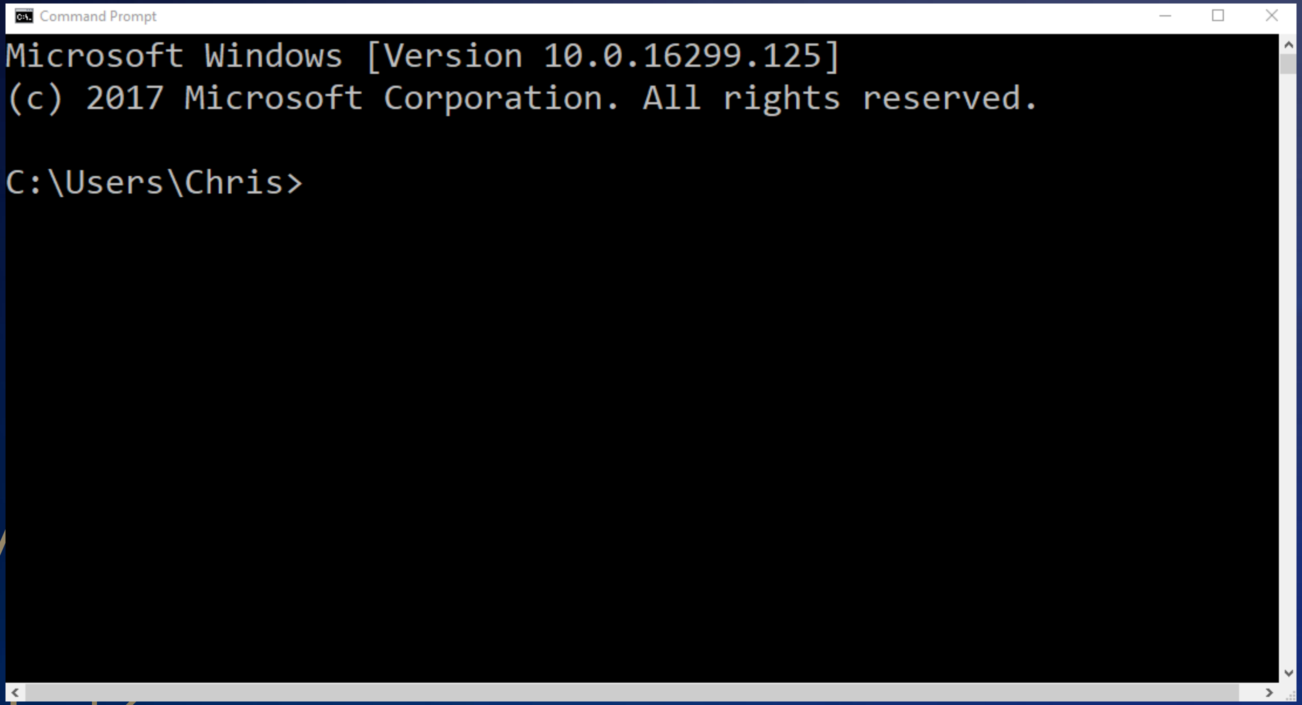
AUDITING WINDOWS SYSTEMS

- “The key to a successful audit of Windows servers is to review the host thoroughly by itself and in conjunction with the many other possible connections that pass data to and from the host.”

WINDOWS COMMAND-LINE

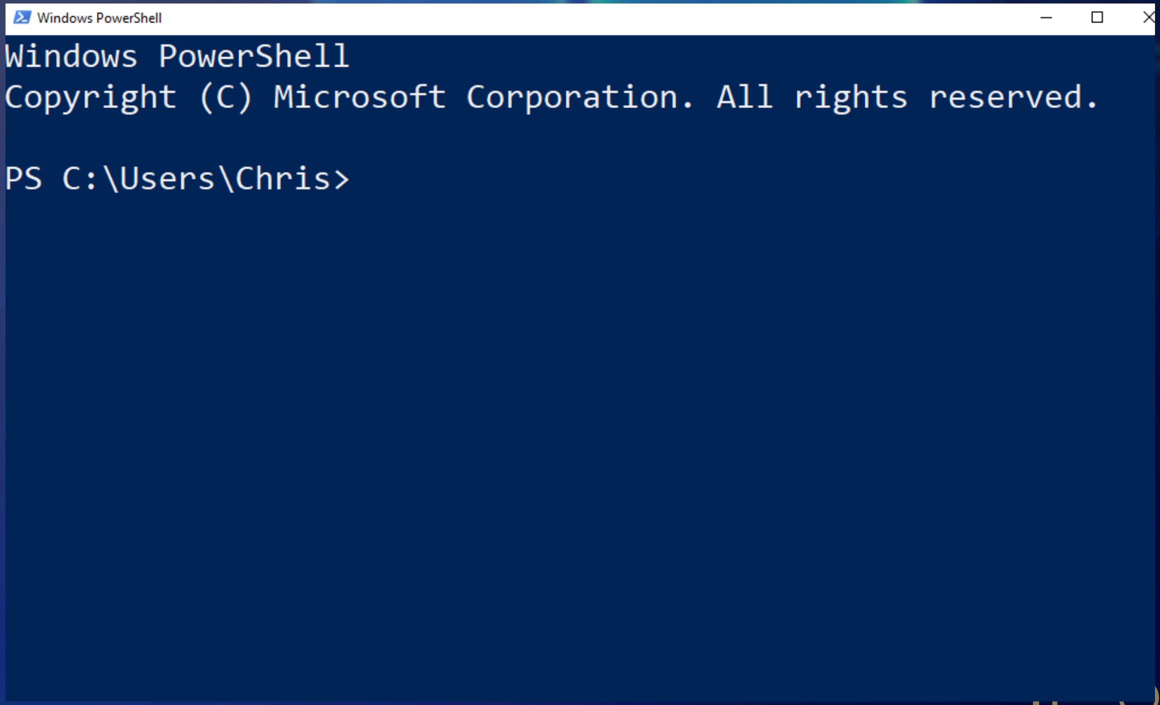
Command Prompt (cmd)

Windows PowerShell



```
Microsoft Windows [Version 10.0.16299.125]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\Chris>
```



```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Chris>
```

SYSINTERNALS

- The Sysinternals tools have been used by administrators for over two decades. The package was so popular that Microsoft bought the suite in 2006. Sysinternals helps administrators and auditors perform complex tasks and detailed analysis.
- Sysinternals suite is a bundling of the following selected Sysinternals Utilities:
  - AccessChk, AccessEnum, AdExplorer, AdInsight, AdRestore, Autologon, Autoruns, BgInfo, BlueScreen, CacheSet, ClockRes, Contig, Coreinfo, Ctrl2Cap, DebugView, Desktops, Disk2vhd, DiskExt, DiskMon, DiskView, Disk Usage (DU), EFSDump, FindLinks, Handle, Hex2dec, Junction, LDMDump, ListDLLs, LiveKd, LoadOrder, LogonSessions, MoveFile, NotMyFault, NTFSInfo, PendMoves, PipeList, PortMon, ProcDump, Process Explorer, Process Monitor, PsExec, PsFile, PsGetSid, PsInfo, PsKill, PsList, PsLoggedOn, PsLogList, PsPasswd, PsPing, PsService, PsShutdown, PsSuspend, PsTools, RAMMap, RDCMan, RegDelNull, RegHide, RegJump, Registry Usage (RU), SDelete, ShareEnum, ShellRunas, Sigcheck, Streams, Strings, Sync, Sysmon, TCPView, VMMap, VolumeID, WhoIs, WinObj, ZoomIt

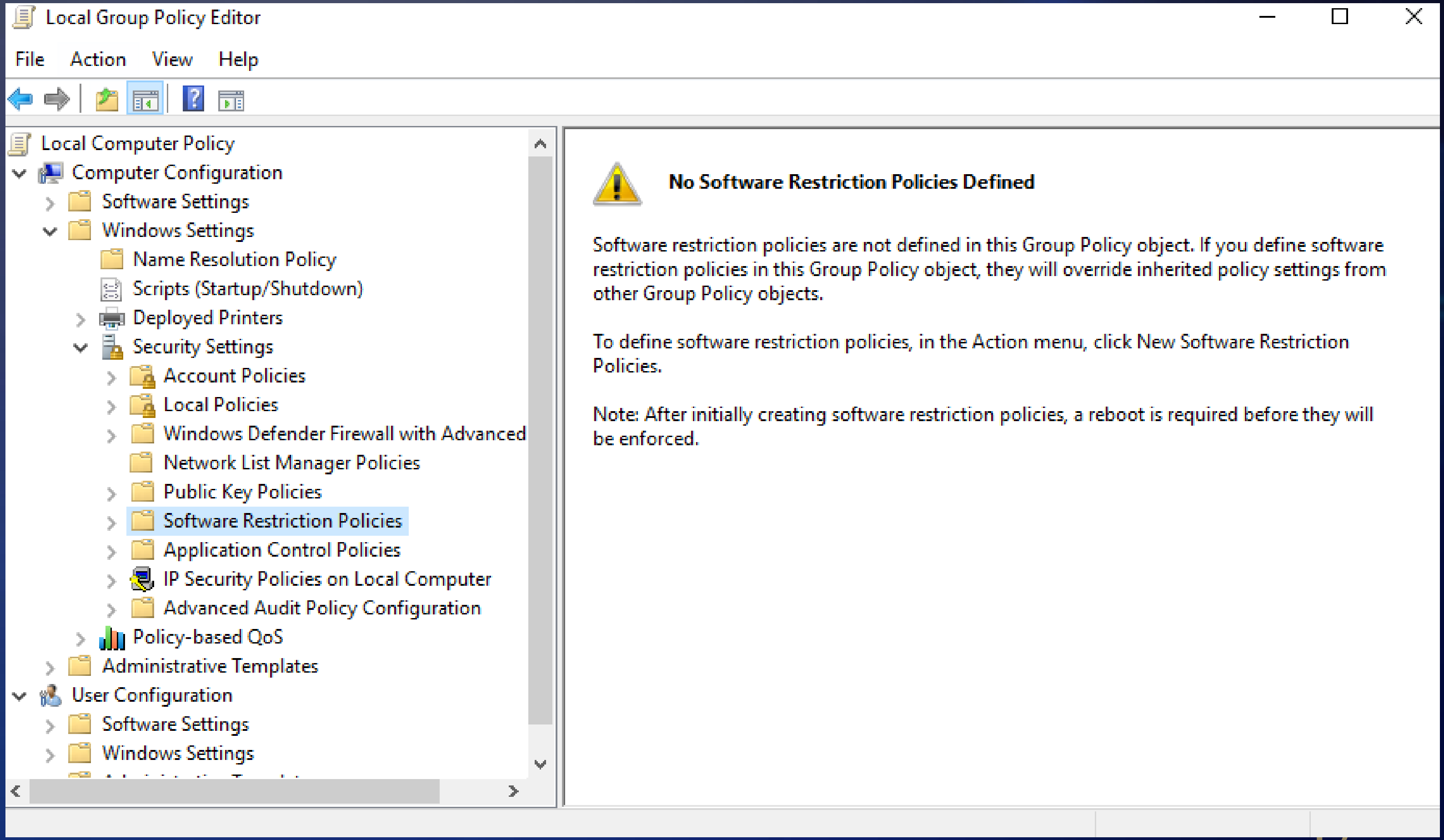
WINDOWS LOCAL SECURITY POLICY

- Secpol.msc
- Renaming guest and administrator accounts
  - Disabling the guest account
  - Choosing not to display the last logged-on user
  - Prompting the user to change the password before expiration
  - Refusing enumeration of SAM accounts and shares by anonymous
  - Refusing to store network credentials (be careful with this!)

- Common user rights assignments include the following:
  - Changing who can access the computer across the network
  - Defining who can log on locally
  - Denying access to the computer from the network
  - Denying logon through terminal services
  - Defining who can take ownership of files or other objects

WINDOWS GROUP POLICY

- **Gpedit.msc**
- **Allows administrators to enforce local policies to multiple systems, through an active directory domain controller**



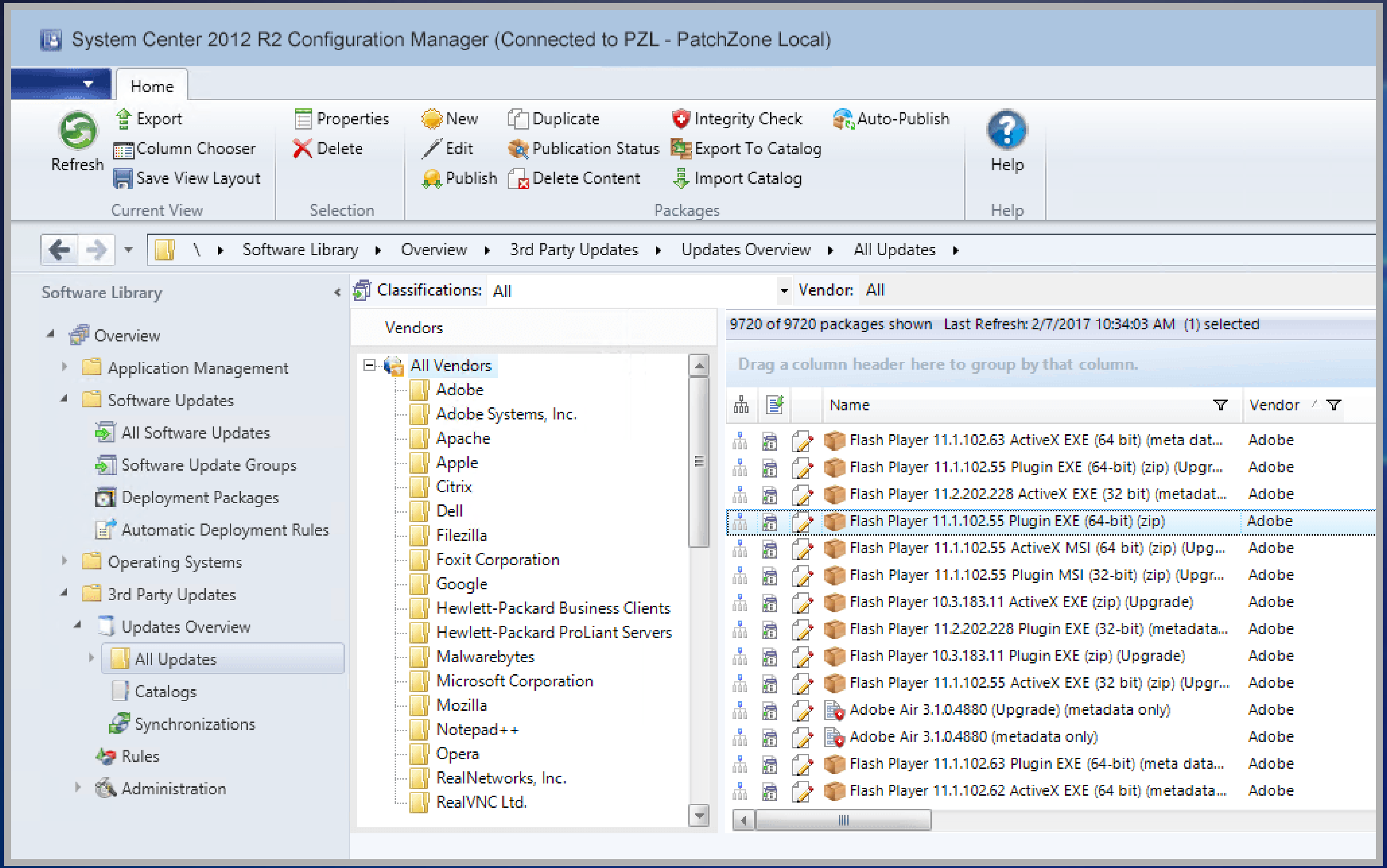
No Software Restriction Policies Defined

Software restriction policies are not defined in this Group Policy object. If you define software restriction policies in this Group Policy object, they will override inherited policy settings from other Group Policy objects.

To define software restriction policies, in the Action menu, click New Software Restriction Policies.

Note: After initially creating software restriction policies, a reboot is required before they will be enforced.

MICROSOFT SYSTEM CENTER CONFIGURATION MANAGER (SCCM)



Classifications: All

Vendor: All

Vendors

- All Vendors
  - Adobe
  - Adobe Systems, Inc.
  - Apache
  - Apple
  - Citrix
  - Dell
  - Filezilla
  - Foxit Corporation
  - Google
  - Hewlett-Packard Business Clients
  - Hewlett-Packard ProLiant Servers
  - Malwarebytes
  - Microsoft Corporation
  - Mozilla
  - Notepad++
  - Opera
  - RealNetworks, Inc.
  - RealVNC Ltd.

9720 of 9720 packages shown   Last Refresh: 2/7/2017 10:34:03 AM   (1) selected

Drag a column header here to group by that column.

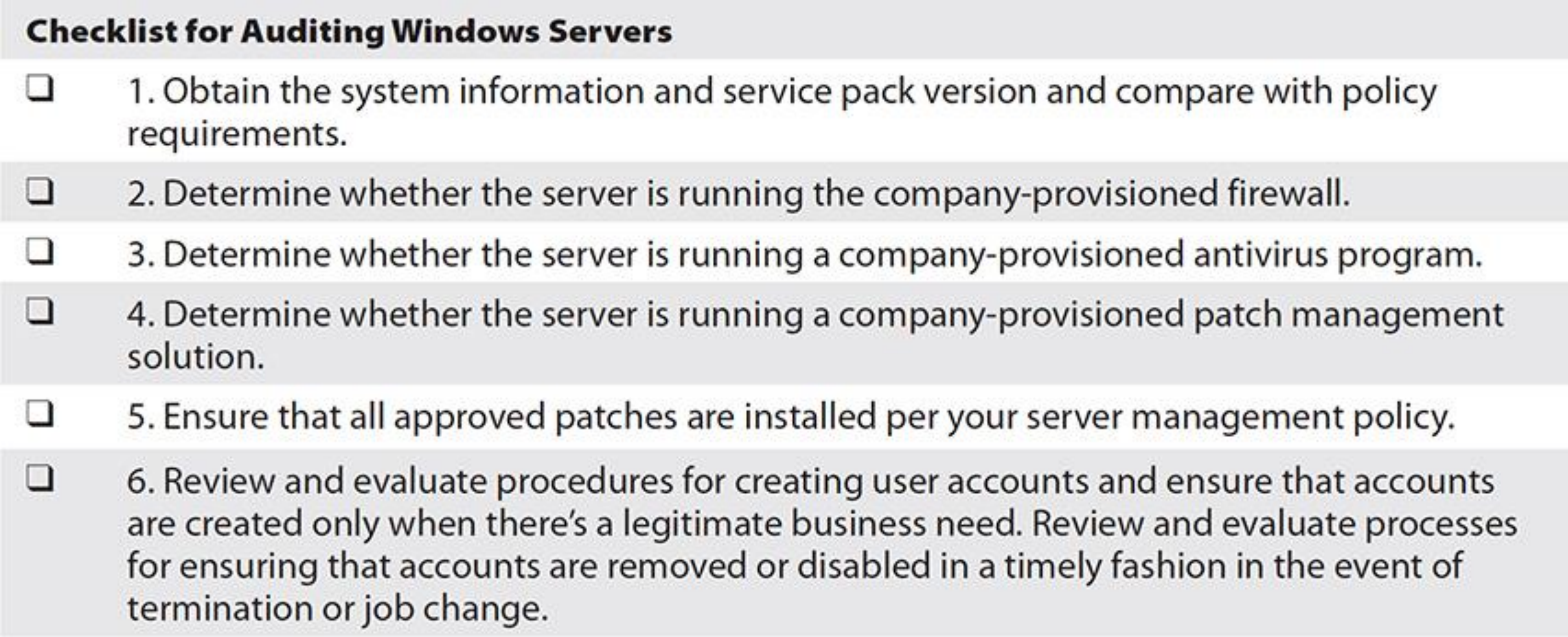
Name	Vendor
Flash Player 11.1.102.63 ActiveX EXE (64 bit) (meta dat...	Adobe
Flash Player 11.1.102.55 Plugin EXE (64-bit) (zip) (Upgr...	Adobe
Flash Player 11.2.202.228 ActiveX EXE (32 bit) (metadat...	Adobe
Flash Player 11.1.102.55 Plugin EXE (64-bit) (zip)	Adobe
Flash Player 11.1.102.55 ActiveX MSI (64 bit) (zip) (Upg...	Adobe
Flash Player 11.1.102.55 Plugin MSI (32-bit) (zip) (Upgr...	Adobe
Flash Player 10.3.183.11 ActiveX EXE (zip) (Upgrade)	Adobe
Flash Player 11.2.202.228 Plugin EXE (32-bit) (metadata...	Adobe
Flash Player 10.3.183.11 Plugin EXE (zip) (Upgrade)	Adobe
Flash Player 11.1.102.55 ActiveX EXE (32 bit) (zip) (Upgr...	Adobe
Adobe Air 3.1.0.4880 (Upgrade) (metadata only)	Adobe
Adobe Air 3.1.0.4880 (metadata only)	Adobe
Flash Player 11.1.102.63 Plugin EXE (64-bit) (meta data...	Adobe
Flash Player 11.1.102.62 ActiveX EXE (64 bit) (metadata...	Adobe

Microsoft® System Center Configuration Manager

REMOTE SERVER ADMINISTRATION TOOLS (RSAT)

- Remote Server Administration Tools (RSAT) enable a Windows 10 client to manage roles and features running on Windows Server systems. RSAT allows administrators to perform remote server management functions and includes several great tools that are otherwise difficult to duplicate in functionality.

GENERAL STEPS FOR AUDITING WINDOWS SYSTEMS



Checklist for Auditing Windows Servers

□ 1. Obtain the system information and service pack version and compare with policy requirements.

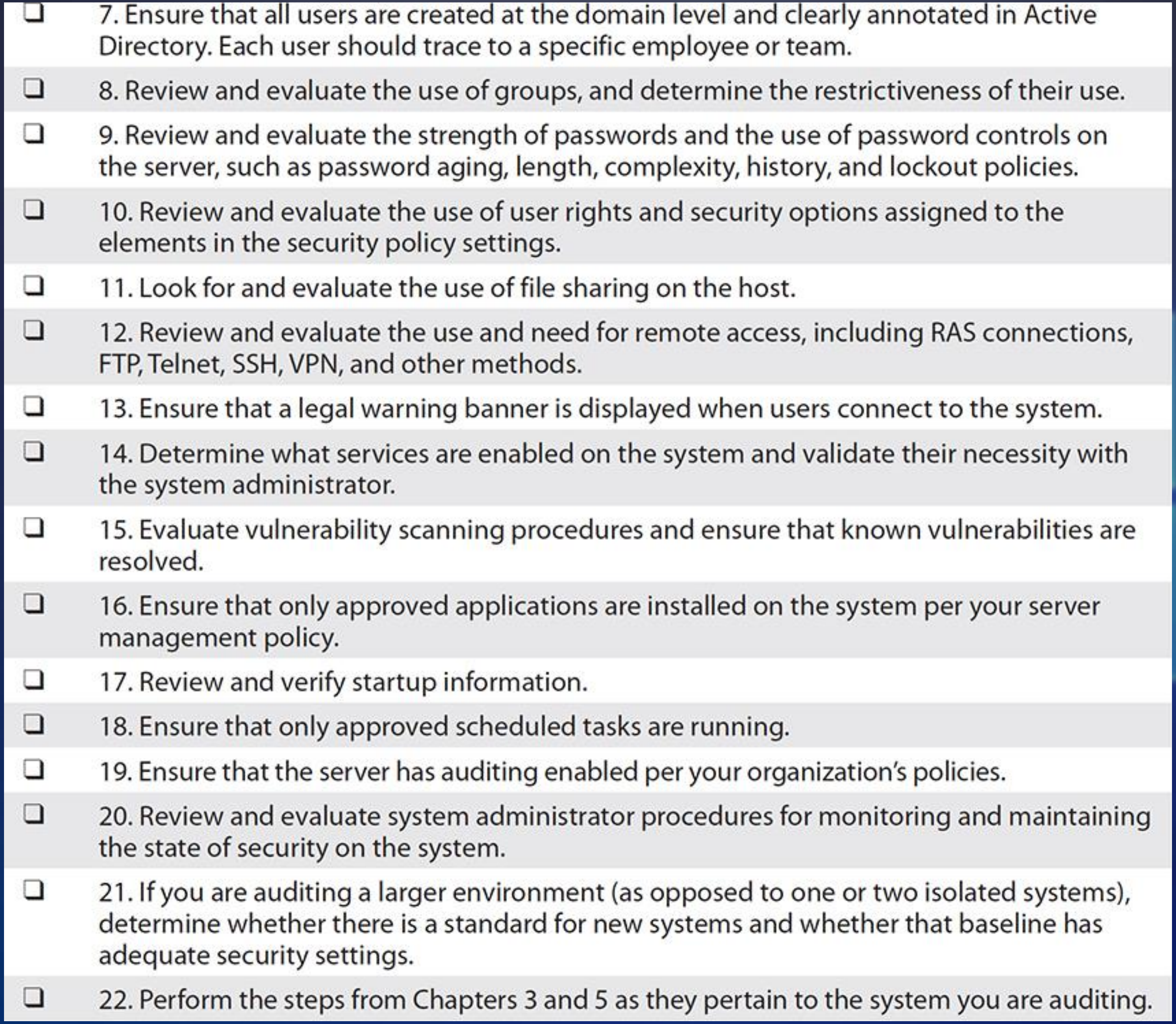
□ 2. Determine whether the server is running the company-provisioned firewall.

□ 3. Determine whether the server is running a company-provisioned antivirus program.

□ 4. Determine whether the server is running a company-provisioned patch management solution.

□ 5. Ensure that all approved patches are installed per your server management policy.

□ 6. Review and evaluate procedures for creating user accounts and ensure that accounts are created only when there's a legitimate business need. Review and evaluate processes for ensuring that accounts are removed or disabled in a timely fashion in the event of termination or job change.



□ 7. Ensure that all users are created at the domain level and clearly annotated in Active Directory. Each user should trace to a specific employee or team.

□ 8. Review and evaluate the use of groups, and determine the restrictiveness of their use.

□ 9. Review and evaluate the strength of passwords and the use of password controls on the server, such as password aging, length, complexity, history, and lockout policies.

□ 10. Review and evaluate the use of user rights and security options assigned to the elements in the security policy settings.

□ 11. Look for and evaluate the use of file sharing on the host.

□ 12. Review and evaluate the use and need for remote access, including RAS connections, FTP, Telnet, SSH, VPN, and other methods.

□ 13. Ensure that a legal warning banner is displayed when users connect to the system.

□ 14. Determine what services are enabled on the system and validate their necessity with the system administrator.

□ 15. Evaluate vulnerability scanning procedures and ensure that known vulnerabilities are resolved.

□ 16. Ensure that only approved applications are installed on the system per your server management policy.

□ 17. Review and verify startup information.

□ 18. Ensure that only approved scheduled tasks are running.

□ 19. Ensure that the server has auditing enabled per your organization’s policies.

□ 20. Review and evaluate system administrator procedures for monitoring and maintaining the state of security on the system.

□ 21. If you are auditing a larger environment (as opposed to one or two isolated systems), determine whether there is a standard for new systems and whether that baseline has adequate security settings.

□ 22. Perform the steps from Chapters 3 and 5 as they pertain to the system you are auditing.