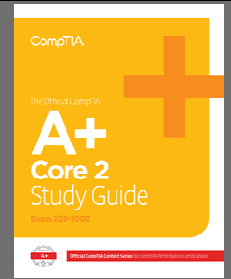
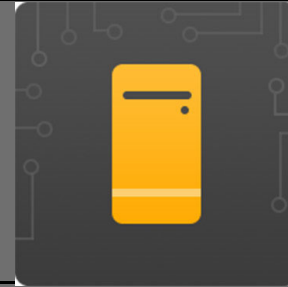


The TestOut PC Pro course and certification exam cover the following CompTIA A+ Certification 220-1002

**TestOut PC Pro v6.0.x
ISBN: 978-1-935080-42-8
Only content that maps to the Exam 220-1002.**

**The Official
CompTIA A+ Core
2 Study Guide**



#	Domain	Resource	Topic
1	Operating Systems		
1.1	Compare and contrast common operating system types and their purposes.		
	32-bit vs. 64-bit		1A
	RAM limitations	3.5.2 CPU Facts	1A
	Software compatibility	3.5.2 CPU Facts	1A
	Workstation operating systems	10.2.1 Windows Versions	1A
	Microsoft Windows	1.3.3 Use the Windows 10 Interface 10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
	Apple Macintosh OS	1.5.1 macOS Introduction 10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
	Linux	1.4.1 Linux Operating Systems 10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
	Cell phone/tablet operating systems		1A
	Microsoft Windows	9.5.1 Mobile Device Overview 9.5.2 Mobile Device Facts	1A
	Android	9.5.1 Mobile Device Overview 9.5.2 Mobile Device Facts	1A
	iOS	9.5.1 Mobile Device Overview 9.5.2 Mobile Device Facts	1A
	Chrome OS	9.5.1 Mobile Device Overview 9.5.2 Mobile Device Facts	1A
	Vendor-specific limitations	12.10.2 Use Windows Update 12.10.3 Update Facts	1A
	End-of-life	12.10.2 Use Windows Update 12.10.3 Update Facts 12.10.5 Update Linux 12.10.6 Update macOS	1A
	Update limitations	12.10.2 Use Windows Update 12.10.3 Update Facts 12.10.5 Update Linux 12.10.6 Update macOS	1A
	Compatibility concerns between operating systems	10.2.5 Verify System Compatibility	1A
1.2	Compare and contrast features of Microsoft Windows versions.		1A
	Windows 7	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A

Windows 8	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
Windows 8.1	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
Windows 10	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
Corporate vs. personal needs	10.2.1 Windows Versions	1A
Domain access	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
Bitlocker	13.8.5 BitLocker 13.8.6 BitLocker Facts 13.8.7 Use BitLocker	1A
Media center	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
Branchcache	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
EFS	13.8.1 File Encryption 13.8.2 File Encryption Facts 13.8.3 Encrypt Files 13.8.4 Configure File Encrvotion	1A
Desktop styles/user interface	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	1A
1.3 Summarize general OS installation considerations and upgrade methods.		
Boot methods	10.3.2 Prepare Disks for Installation	2C
USB	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
CD-ROM	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
DVD	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
PXE	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
Solid state/flash drives	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
Netboot	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
External/hot-swappable drive	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
Internal hard drive (partition)	10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
Type of installations	10.2.3 Pre-Installation Planning	2C
Unattended installation	10.2.3 Pre-Installation Planning	2C
In-place upgrade	10.2.3 Pre-Installation Planning	2C

Clean install	10.2.3 Pre-Installation Planning	2C
Repair installation	10.2.3 Pre-Installation Planning	2C
Multiboot	10.2.3 Pre-Installation Planning	2C
Remote network installation	10.2.3 Pre-Installation Planning	2C
Image deployment	10.2.3 Pre-Installation Planning	2C
Recovery partition	10.2.3 Pre-Installation Planning	2C
Refresh/restore	10.2.3 Pre-Installation Planning	2C
Partitioning		1E
Dynamic	5.5.4 MBR Partitioning 5.5.5 MBR Partitioning Facts 5.6.1 Create Volumes with Disk Management	1E
Basic	5.5.4 MBR Partitioning 5.5.5 MBR Partitioning Facts 5.6.1 Create Volumes with Disk Management	1E
Primary	5.5.4 MBR Partitioning 5.5.5 MBR Partitioning Facts 5.6.1 Create Volumes with Disk Management	1E
Extended	5.5.4 MBR Partitioning 5.5.5 MBR Partitioning Facts 5.6.1 Create Volumes with Disk Management	1E
Logical	5.5.4 MBR Partitioning 5.5.5 MBR Partitioning Facts 5.6.1 Create Volumes with Disk Management	1E
GPT	5.5.6 GPT Partitioning 5.5.7 GPT Partitioning Facts	1E
File system types/formatting	12.11.5 Use Time Machine on macOS	1E, 2A, 2B
ExFAT	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	1E
FAT32	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	1E
NTFS	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	1E
CDFS	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	1E
NFS	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	2A
ext3, ext4	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	2A
HFS	1.5.1 macOS Introduction 12.11.5 Use Time Machine on macOS	2B
Swap partition	13.2.2 Basic Forensic Procedures	2A
Quick format vs. full format	5.5.1 Partitions, Volumes, and File Systems 5.5.3 File System Facts	1E
Load alternate third-party drivers when necessary	10.3.4 Install Windows	2C
Workgroup vs. Domain setup	11.4.3 Configure Advanced Folder Sharing on Windows	2C
Time/date/region/language settings	10.3.4 Install Windows	2C
Driver installation, software, and Windows updates	10.3.4 Install Windows	2C
Factory recovery partition	10.3.4 Install Windows	2C
Properly formatted boot drive with the correct partitions/format	10.2.3 Pre-Installation Planning 10.3.1 Windows Installation 10.3.2 Prepare Disks for Installation	2C

	Prerequisites/hardware compatibility	10.2.3 Pre-Installation Planning 10.2.4 Installation Planning Facts 10.2.5 Verify System Compatibility	2C
	Application compatibility	12.14.4 Application Troubleshooting Facts	2C
	OS compatibility/upgrade path	10.2.5 Verify System Compatibility 12.10.2 Use Windows Update 12.10.5 Update Linux 12.10.6 Update macOS	2C
1.4	Given a scenario, use appropriate Microsoft command line tools.		
	Navigation	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
	dir	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
	cd..	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
	ipconfig	6.9.1 Network Utilities 6.9.2 Use ipconfig and ifconfig 6.9.3 Explore Configuration Information 16.9.4 Explore Configuration Information 2 6.9.5 Explore Configuration Information 3 6.9.9 TCP/IP Utilities 11.2.8 File Management Commands	4E
	ping	6.9.1 Network Utilities 6.9.2 Use ipconfig and ifconfig 6.9.3 Explore Configuration Information 1 6.9.4 Explore Configuration Information 2 6.9.5 Explore Configuration Information 3 6.9.7 Use ping and tracert 6.9.9 TCP/IP Utilities	4E
	tracert	6.9.1 Network Utilities 6.9.2 Use ipconfig and ifconfig 6.9.3 Explore Configuration Information 1 6.9.4 Explore Configuration Information 2 6.9.5 Explore Configuration Information 3 6.9.7 Use ping and tracert 6.9.9 TCP/IP Utilities	4E
	netstat	6.9.1 Network Utilities 6.9.2 Use ipconfig and ifconfig 6.9.3 Explore Configuration Information 1 6.9.4 Explore Configuration Information 2 6.9.5 Explore Configuration Information 3 6.9.9 TCP/IP Utilities	4E

	nslookup	6.9.1 Network Utilities 6.9.2 Use ipconfig and ifconfig 6.9.3 Explore Configuration Information 1 6.9.4 Explore Configuration Information 2 6.9.5 Explore Configuration Information 3 6.9.8 Use nslookup 6.9.9 TCP/IP Utilities	4E
	shutdown	12.1.11 Explore System Commands 12.1.13 Use System Commands	1C
	dism	10.3.2 Prepare Disks for Installation 10.3.4 Install Windows	2C
	sfc	12.15.8 Startup Error Facts	3C
	chkdsk	5.9.5 Disk Optimization Facts	6D
	diskpart	5.6.2 Create Volumes with Diskpart	1E
	taskkill	12.1.11 Explore System Commands 12.1.13 Use System Commands	3A
	gpupdate	5.6.1 Create Volumes with Disk Management 12.1.13 Use System Commands	5C
	gpresult	12.1.13 Use System Commands	5C
	format	5.6.3 Create Volumes 5.6.4 Convert Volumes 5.6.5 Format Drives	1E
	copy	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands	1D
	xcopy	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands	1D
	robocopy	11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands	1D
	net use	11.4.1 Shared Folders 11.4.3 Configure Advanced Folder Sharing on Windows 11.4.5 Shared Folder Facts	5B
	net user	12.5.1 Users and Groups 12.5.2 Manage Local Users and Groups 12.5.3 User and Group Facts	5A
	[command name] /?	12.1.11 Explore System Commands 12.1.13 Use System Commands	1C
	Commands available with standard privileges vs. administrative privileges	12.1.11 Explore System Commands 12.1.13 Use System Commands	1A
1.5	Given a scenario, use Microsoft operating system features and tools. Administrative	12.1.6 Management Consoles Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.5.7 Manage UAC Settings 12.5.8 UAC Facts 12.7.6 Schedule Tasks	1C, 1F, 3A, 3B, 3C, 4C, 4D, 5A

Computer Management	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	1C
Device Manager	4.5.3 Manage Device Drivers on Windows 4.5.8 Manage Devices 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	1F
Local Users and Groups	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	5A
Local Security Policy	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	5A

Performance Monitor	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	3B
Services	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	3A
System Configuration	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	3C
Task Scheduler	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	6D

Component Services	<ul style="list-style-type: none"> 4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows 	3A
Data Sources	<ul style="list-style-type: none"> 4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows 	3A
Print Management	<ul style="list-style-type: none"> 4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows 	3A
Windows Memory Diagnostics	<ul style="list-style-type: none"> 3.9.2 Test Memory 4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows 	3C

Windows Firewall	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	4C
Advanced Security	4.5.3 Manage Device Drivers on Windows 4.6.2 Troubleshoot Devices 8.4.2 Manage Print Jobs 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.10 Windows Utilities Facts 12.3.2 Monitor System Performance 12.5.2 Manage Local Users and Groups 12.7.6 Schedule Tasks 13.7.3 Configure Password Policies on Windows	4C
Event Viewer	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information	3C
User Account Management	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.5.6 Manage Users and Groups 12.5.7 Manage UAC Settings 12.5.8 UAC Facts	1C
MSConfig		3C
General	12.1.7 View System Information 12.1.10 Windows Utilities Facts	3C
Boot	12.1.7 View System Information 12.1.10 Windows Utilities Facts	3C
Services	12.1.7 View System Information 12.1.10 Windows Utilities Facts	3C
Startup	12.1.7 View System Information 12.1.10 Windows Utilities Facts	3C
Tools	12.1.7 View System Information 12.1.10 Windows Utilities Facts	3C
Task Manager	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A
Applications	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A
Processes	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A

Performance	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A
Networking	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A
Users	12.1.1 Use Task Manager 12.1.2 Task Manager Facts	3A
Disk Management		1E
Drive status	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Mounting	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Initializing	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Extending partitions	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E

Splitting partitions	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Shrink partitions	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Assigning/changing drive letters	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Adding drives	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
Adding arrays	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E

Storage spaces	5.6.1 Create Volumes with Disk Management 5.6.2 Create Volumes with Diskpart 5.6.3 Create Volumes 5.6.4 Convert Volumes 5.7.2 Create Mount Points and Extending Volumes 5.7.3 Shrink and Split Partitions 5.8.1 Storage Spaces 5.8.2 Create Storage Spaces 5.8.2 Storage Space Facts	1E
System utilities	12.1.6 Management Consoles Facts 12.10.2 Use Windows Update	1C, 1D, 1F, 6D, 3A, 3C
Regedit	5.9.1 Storage Optimization 5.9.2 Optimize Disks in Windows 5.9.3 Optimize Disks in Linux 5.9.4 Optimize Disks in macOS 5.9.5 Disk Optimization Facts 11.4.1 Shared Folders 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update	1C
Command	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.12.2 Use Restore Points	1C
Services.msc	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.12.2 Use Restore Points	3A

MMC	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.1.2 Use Restore Points	1C
MSTSC	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.1.2 Use Restore Points	4D
Notepad	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.1.2 Use Restore Points	1C
Explorer	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.1.2 Use Restore Points	1D
Msinfo32	5.9.1 Storage Optimization 5.9.2 Optimize Disks in Windows 5.9.3 Optimize Disks in Linux 5.9.4 Optimize Disks in macOS 5.9.5 Disk Optimization Facts 11.4.1 Shared Folders 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update	1F

DxDiag	5.9.1 Storage Optimization 5.9.2 Optimize Disks in Windows 5.9.3 Optimize Disks in Linux 5.9.4 Optimize Disks in macOS 5.9.5 Disk Optimization Facts 11.4.1 Shared Folders 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update	1F
Disk Defragmenter	5.9.1 Storage Optimization 5.9.2 Optimize Disks in Windows 5.9.3 Optimize Disks in Linux 5.9.4 Optimize Disks in macOS 5.9.5 Disk Optimization Facts 11.4.1 Shared Folders 12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore SystemCommands 12.1.13 Use SystemCommands 12.10.2 Use WindowsUpdate	6D
System Restore	12.1.5 Use Management 12.1.5 Use ManagementConsoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows Utilities Facts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use WindowsUpdate 12.12.2 Use Restore Points	3C
Windows Update	12.1.5 Use Management Consoles 12.1.6 Management Consoles Facts 12.1.7 View System Information 12.1.9 Use Regedit 12.1.10 Windows UtilitiesFacts 12.1.11 Explore System Commands 12.1.13 Use System Commands 12.10.2 Use Windows Update 12.12.2 Use Restore Points	6D
1.6 Given a scenario, use Microsoft Windows Control Panel utilities. Internet Options		4C

Connections		4C
Security		4C
General		4C
Privacy		4C
Programs		4C
Advanced		4C
Display/Display Settings		1F
Resolution	4.3.1 Configure Display Settings in Windows 4.3.2 Configure Advanced Display Settings in Windows 4.3.6 Display Device Facts	1F
Color depth	4.3.1 Configure Display Settings in Windows 4.3.2 Configure Advanced Display Settings in Windows 4.3.6 Display Device Facts	1F
Refresh rate	4.3.1 Configure Display Settings in Windows 4.3.2 Configure Advanced Display Settings in Windows 4.3.6 Display Device Facts	1F
User Accounts	12.5.2 Manage Local Users and Groups	1C
Folder Options		1D
View hidden files	11.2.4 Manage Files on Windows 11.2.5 Manage Files 11.2.6 Manage Directories from the Command Prompt 11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
Hide extensions	11.2.4 Manage Files on Windows 11.2.5 Manage Files 11.2.6 Manage Directories from the Command Prompt 11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
General options	11.2.4 Manage Files on Windows 11.2.5 Manage Files 11.2.6 Manage Directories from the Command Prompt 11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
View options	11.2.4 Manage Files on Windows 11.2.5 Manage Files 11.2.6 Manage Directories from the Command Prompt 11.2.7 Manage Files from the Command Prompt 11.2.8 File Management Commands 11.2.9 Manage Files and Folders	1D
System	12.6.2 Use Remote Desktop 12.13.2 Manage the Paging File	3B
Performance (virtual memory)	12.6.2 Use Remote Desktop 12.12.2 Use Restore Points 12.13.2 Manage the Paging File	3B
Remote settings	12.6.2 Use Remote Desktop 12.12.2 Use Restore Points 12.13.2 Manage the Paging File	3B

	System protection	12.6.2 Use Remote Desktop 12.12.2 Use Restore Points 12.13.2 Manage the Paging File	3B
	Windows Firewall	13.10.2 Configure Windows Firewall	4C
	Power Options		1F
	Hibernate	9.3.3 Configure Power Options	1F
	Power plans	9.3.3 Configure Power Options	1F
	Sleep/suspend	9.3.3 Configure Power Options	1F
	Standby	9.3.3 Configure Power Options	1F
	Credential Manager	13.7.8 Use a Biometric Scanner	5A
	Programs and features	12.7.2 Manage Windows Desktop Applications	3A
	HomeGroup	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	5B
	Devices and Printers	8.2.2 Install a Local Printer 8.2.4 Printer Configuration Facts	1F
	Sound	3.13.4 Manage Audio Devices	1F
	Troubleshooting	12.1.3 Use Control Panel 12.1.4 Control Panel Facts	1F
	Network and Sharing Center	6.6.3 Configure TCP/IP Properties	4A
	Device Manager	4.5.8 Manage Devices	1F
	BitLocker	13.8.5 BitLocker 13.8.6 BitLocker Facts 13.8.7 Use BitLocker	7B
	Sync Center	12.1.3 Use Control Panel 12.1.4 Control Panel Facts	5B
1.7	Summarize application installation and configuration concepts.		
	System requirements		3A
	Drive space		3A
	RAM	3.7.1 Random Access Memory 3.7.2 DRAM Types 3.7.3 RAM Facts 5.6.3 Create Volumes	3A
	OS requirements	10.2.5 Verify System Compatibility 12.10.2 Use Windows Update	3A
	Compatibility	10.2.5 Verify System Compatibility 12.10.2 Use Windows Update 12.10.5 Update Linux 12.10.6 Update macOS	3A
	Methods of installation and deployment	10.2.4 Installation Planning Facts	3A
	Local (CD/USB)	10.2.4 Installation Planning Facts 10.3.1 Windows Installation	3A
	Network-based	10.2.4 Installation Planning Facts 10.3.1 Windows Installation	3A
	Local user permissions		3A
	Folder/file access for installation	11.3.1 NTFS Permissions 11.3.2 Configure NTFS Permissions 11.3.3 NTFS Permission Facts	3A
	Security considerations		3A
	Impact to device	13.13.1 Common Security Issues	3A
	Impact to network	13.13.1 Common Security Issues	3A
1.8	Given a scenario, configure Microsoft Windows networking on a client/desktop.		

HomeGroup vs. Workgroup	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	5B
Domain setup	10.2.1 Windows Versions 10.2.2 Windows Versions Facts	5C
Network shares/administrative shares/mapping drives	11.4.1 Shared Folders 11.4.2 Configure Basic Folder Sharing on Windows 11.4.3 Configure Advanced Folder Sharing on Windows 11.4.4 Configure Share and NTFS Permissions 11.4.5 Shared Folder Facts 11.4.6 Share and Secure Folders	5B
Printer sharing vs. network printer mapping	8.3.1 Network Printing 8.3.2 Share a Printer 8.3.4 Network Printing Facts 8.3.5 Configure Network Printing	5B
Establish networking connections	6.4.1 Ethernet 6.4.2 Ethernet Facts 6.4.3 Ethernet Standards 6.8.1 Internet Services 6.8.2 Internet Connection Facts 7.1.3 Wireless Networking Facts 7.1.5 Wireless Security Facts	4A
VPN	13.12.1 Virtual Private Networks (VPN) 13.12.2 Set Up a VPN Connection 13.12.3 VPN Facts 13.12.4 Configure a VPN Connection	4A
Dial-ups	6.8.5 Create a Dial-up Internet Connection 6.8.6 Configure a Dial-up Internet Connection	4A
Wireless	7.1.1 Wireless Networking 7.1.2 Install a Wireless Network Adapter 7.1.3 Wireless Networking Facts 7.1.4 Wireless Security 7.1.5 Wireless Security Facts 7.1.5 Wireless Security Facts 7.1.6 Configure a Wireless Connection 7.1.7 Connect to a Wireless Network 7.1.8 Create a Home Wireless Network 7.1.9 Secure Home Wireless Network 7.1.10 Configure Wireless Profiles	4A
Wired	6.8.1 Internet Services 6.8.2 Internet Connection Facts 6.8.3 Configure a Cable Internet Connection 6.8.4 Configure a DSL Internet Connection 6.8.5 Create a Dial-up Internet Connection 6.8.6 Configure a Dial-up Internet Connection	4A
WWAN (Cellular)	6.4.1 Ethernet 6.4.2 Ethernet Facts 6.4.3 Ethernet Standards	4A
Proxy settings	13.11.1 Proxy Settings 13.11.2 Configure Proxy Settings 13.11.3 Proxy Server Facts 13.11.4 Use a Proxy Server	4C

Remote Desktop Connection	12.6.1 Remote Desktop 12.6.2 Use Remote Desktop 12.6.3 Remote Desktop Facts 12.6.4 Remote Assistance 12.6.5 Remote Assistance Facts 12.6.6 Use Remote Assistance 12.6.7 Configure Remote Services	4D
Remote Assistance	12.6.1 Remote Desktop 12.6.2 Use Remote Desktop 12.6.3 Remote Desktop Facts 12.6.4 Remote Assistance 12.6.5 Remote Assistance Facts 12.6.6 Use Remote Assistance 12.6.7 Configure Remote Services	4D
Home vs. Work vs. Public network settings		4C
Firewall settings		4C
Exceptions	13.10.1 Firewalls 13.10.2 Configure Windows Firewall 13.10.3 Firewall Facts 13.10.4 Configure a Windows Firewall	4C
Configuration	13.10.1 Firewalls 13.10.2 Configure Windows Firewall 13.10.3 Firewall Facts 13.10.4 Configure a Windows Firewall	4C
Enabling/disabling Windows Firewall	13.10.1 Firewalls 13.10.2 Configure Windows Firewall 13.10.3 Firewall Facts 13.10.4 Configure a Windows Firewall	4C
Configuring an alternative IP address in Windows	6.6.1 IP Configuration 6.6.2 TCP/IP Configuration Methods 6.6.3 Configure TCP/IP Properties 6.6.4 IP Configuration Facts	4A
IP addressing	6.6.1 IP Configuration 6.6.2 TCP/IP Configuration Methods 6.6.3 Configure TCP/IP Properties 6.6.4 IP Configuration Facts 6.6.5 Configure TCP/IP Settings 6.6.6 Configure Alternate TCP/IP Settings	4A
Subnet mask	6.6.1 IP Configuration 6.6.2 TCP/IP Configuration Methods 6.6.3 Configure TCP/IP Properties 6.6.4 IP Configuration Facts 6.6.5 Configure TCP/IP Settings 6.6.6 Configure Alternate TCP/IP Settings	4A
DNS	6.6.1 IP Configuration 6.6.2 TCP/IP Configuration Methods 6.6.3 Configure TCP/IP Properties 6.6.4 IP Configuration Facts 6.6.5 Configure TCP/IP Settings 6.6.6 Configure Alternate TCP/IP Settings	4A

	Gateway	6.6.1 IP Configuration 6.6.2 TCP/IP Configuration Methods 6.6.3 Configure TCP/IP Properties 6.6.4 IP Configuration Facts 6.6.5 Configure TCP/IP Settings 6.6.6 Configure Alternate TCP/IP Settings	4A
	Network card properties	6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts	4A
	Half duplex/full duplex/auto	6.2.1 Network Infrastructure 6.2.2 Network Devices 6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts 6.2.6 Select and Install a Network Adapter	4A
	Speed	6.2.1 Network Infrastructure 6.2.2 Network Devices 6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts 6.2.6 Select and Install a Network Adapter	4A
	Wake-on-LAN	6.2.1 Network Infrastructure 6.2.2 Network Devices 6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts 6.2.6 Select and Install a Network Adapter	4A
	QoS	6.2.1 Network Infrastructure 6.2.2 Network Devices 6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts 6.2.6 Select and Install a Network Adapter	4A
	BIOS (on-board NIC)	6.2.1 Network Infrastructure 6.2.2 Network Devices 6.2.4 Network Infrastructure and Device Facts 6.2.5 Network Adapter Facts 6.2.6 Select and Install a Network Adapter	4A
1.9	Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems.		
	Best practices	12.11.4 Create Backups in Linux 12.11.5 Use Time Machine on macOS	6D
	Scheduled backups	12.11.4 Create Backups in Linux 12.11.5 Use Time Machine on macOS	6D
	Scheduled disk maintenance		6D
	System updates/App Store	12.10.5 Update Linux 12.10.6 Update macOS	6D
	Patch management	12.10.5 Update Linux 12.10.6 Update macOS	6D
	Driver/firmware updates	4.5.4 Manage Devices on Linux 4.5.5 Manage Devices on macOS	6D
	Antivirus/Anti-malware updates	13.6.7 Implement Malware Protection on Linux 13.6.8 Implement Malware Protection on macOS	6D

Tools	12.6.8 Use Screen Sharing 12.6.9 Screen Sharing Facts 12.11.5 Use Time Machine on macOS 12.12.8 Restore Data on Linux 12.12.9 Restore Data on macOS	2B, 6D
Backup/Time Machine	12.11.5 Use Time Machine on macOS	6D
Restore/Snapshot	12.11.5 Use Time Machine on macOS 12.12.8 Restore Data on Linux 12.12.9 Restore Data on macOS	6D
Image recovery	12.12.8 Restore Data on Linux 12.12.9 Restore Data on macOS	2B
Disk maintenance utilities		6D
Shell/Terminal	1.4.1 Linux Operating Systems 1.4.4 Use Shell Commands 1.4.5 Shut Down a Linux System	2B
Screen sharing	12.6.8 Use Screen Sharing 12.6.9 Screen Sharing Facts	2B
		2B
Force Quit	12.8.2 Manage Apps on Linux 12.8.3 Manage Processes on Linux	2B
Features		2B
Multiple desktops/Mission Control	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B
Key Chain	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B
Spot Light	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B
iCloud	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B
Gestures	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.4 macOS Facts	2B
Finder	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B
Remote Disc	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.4 macOS Facts	2B
Dock	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.3 macOS Features and Settings 1.5.4 macOS Facts	2B

Boot Camp	1.5.1 macOS Introduction 1.5.2 Use the macOS Interface 1.5.4 macOS Facts	2B
Basic Linux commands	12.8.4 Linux Application Management Facts	2A
ls	1.4.2 Use Linux Shell Commands 1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
grep	11.5.2 View File Contents	2A
cd	1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
shutdown	1.4.2 Use Linux Shell Commands 1.4.3 Linux Facts 1.4.5 Shut Down a Linux System 11.5.5 Linux File Management Facts	2A
pwd vs. passwd	1.4.2 Use Linux Shell Commands 1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
mv	1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
cp	1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
rm	1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
chmod	11.5.4 Manage Ownership and Permissions 11.5.5 Linux File Management Facts	2A
chown	11.5.4 Manage Ownership and Permissions 11.5.5 Linux File Management Facts	2A
iwconfig/ifconfig	1.4.3 Linux Facts 6.9.2 Use ipconfig and ifconfig 6.9.6 Use ifconfig	2A
ps	12.8.2 Manage Apps on Linux 12.8.3 Manage Processes on Linux	2A
su/sudo	1.4.3 Linux Facts 12.8.1 Install Linux Software	2A
apt-get	12.8.1 Install Linux Software 12.8.4 Linux Application Management Facts	2A
vi	11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A

	dd	1.4.3 Linux Facts 11.5.1 Manage the Linux File System 11.5.3 Edit File Contents 11.5.5 Linux File Management Facts	2A
	kill	12.1.11 Explore System Commands 12.8.5 Manage Linux Processes	2A
2.0 Security			
2.1	Summarize the importance of physical security measures.		6C
	Mantrap	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Badge reader	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Smart card	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Security guard	13.3.7 Physical Security Facts	6C
	Door lock	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Biometric locks	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Hardware tokens	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Cable locks	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Server locks	13.3.7 Physical Security Facts	6C
	USB locks	13.3.7 Physical Security Facts	6C
	Privacy screen	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Key fobs	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
	Entry control roster	13.3.1 Physical Security 13.3.7 Physical Security Facts	6C
2.2	Explain logical security concepts.		
	Active Directory	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.1 Users and Groups 12.5.3 User and Group Facts	5C
	Login script	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts	5C
	Domain	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.3 User and Group Facts	5C

Group Policy/Updates	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.1 Users and Groups	5C
Organizational Units	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts	5C
Home Folder	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts	5C
Folder redirection	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts	5C
Software tokens	13.7.1 Authentication 13.7.4 Password Facts	7A
MDM policies	9.7.2 Mobile Device Security Facts	6A
Port security	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts	6A
MAC address filtering	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts	6A
Certificates	7.1.5 Wireless Security Facts	6A
Antivirus/Anti-malware	13.6.2 Malware Facts 13.6.3 Malware Protection 13.6.4 Implement Malware Protection on Windows	6A
Firewalls	13.10.1 Firewalls 13.10.2 Configure Windows Firewall 13.10.3 Firewall Facts	6A
User authentication/strong passwords	13.7.1 Authentication 13.7.4 Password Facts	7A
Multifactor authentication	13.7.1 Authentication 13.7.4 Password Facts	7A
Directory permissions	13.7.1 Authentication 13.7.4 Password Facts	7B
VPN	13.12.1 Virtual Private Networks (VPN) 13.12.2 Set Up a VPN Connection 13.12.3 VPN Facts 13.12.4 Configure a VPN Connection	6A
DLP	13.3.2 Data Disposal and Destruction	7B
Access control lists	13.3.1 Physical Security	6A
Smart card	13.7.1 Authentication 13.7.4 Password Facts	6C
Email filtering	13.10.5 Network Appliances 13.10.6 Network Appliance Facts	8B

	Trusted/untrusted software sources	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts	6A
	Principle of least privilege	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts	6A
2.3	Compare and contrast wireless security protocols and authentication methods.		
	Protocols and encryption	7.1.5 Wireless Security Facts	4B
	WEP	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	4B
	WPA	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	4B
	WPA2	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	4B
	TKIP	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	4B
	AES	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	4B
	Authentication	7.1.5 Wireless Security Facts	7A
	Single-factor	13.7.1 Authentication 13.7.4 Password Facts	7A
	Multifactor	13.7.1 Authentication 13.7.4 Password Facts	7A
	RADIUS	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	7A
	TACACS	7.1.4 Wireless Security 7.1.5 Wireless Security Facts	7A
2.4	Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.		
	Malware		8A
	Ransomware	13.6.1 Malware 13.6.2 Malware Facts	8A
	Trojan	13.6.1 Malware 13.6.2 Malware Facts	8A
	Keylogger	13.6.1 Malware 13.6.2 Malware Facts	8A
	Rootkit	13.6.1 Malware 13.6.2 Malware Facts	8A
	Virus	13.6.1 Malware 13.6.2 Malware Facts	8A
	Botnet	13.6.1 Malware 13.6.2 Malware Facts	8A
	Worm	13.6.1 Malware 13.6.2 Malware Facts	8A
	Spyware	13.6.1 Malware 13.6.2 Malware Facts	8A
	Tools and methods		8A
	Antivirus	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8A
	Anti-malware	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8A
	Recovery console	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8A

	Backup/restore	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8A
	End user education	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8A
	Software firewalls	13.10.1 Firewalls 13.10.2 Configure Windows Firewall 13.10.3 Firewall Facts	8A
	SecureDNS	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts	8A
2.5	Compare and contrast social engineering, threats, and vulnerabilities.		
	Social engineering		6B
	Phishing	13.6.1 Malware 13.6.2 Malware Facts	6B
	Spear phishing	13.6.1 Malware 13.6.2 Malware Facts	6B
	Impersonation	13.6.1 Malware 13.6.2 Malware Facts	6B
	Shoulder surfing	13.6.1 Malware 13.6.2 Malware Facts	6B
	Tailgating	13.6.1 Malware 13.6.2 Malware Facts	6B
	Dumpster diving	13.6.1 Malware 13.6.2 Malware Facts	6B
	DDoS	13.6.1 Malware 13.6.2 Malware Facts	6B
	DoS	6.9.1 Network Utilities 13.6.1 Malware 13.6.2 Malware Facts	6B
	Zero-day	13.6.1 Malware 13.6.2 Malware Facts	6B
	Man-in-the-middle	13.6.1 Malware 13.6.2 Malware Facts	6B
	Brute force	13.6.1 Malware 13.6.2 Malware Facts	6B
	Dictionary	13.6.1 Malware 13.6.2 Malware Facts	6B
	Rainbow table	13.6.1 Malware 13.6.2 Malware Facts	6B
	Spoofing	13.6.1 Malware 13.6.2 Malware Facts	6B
	Non-compliant systems	13.6.1 Malware 13.6.2 Malware Facts	6B
	Zombie	13.6.1 Malware 13.6.2 Malware Facts	6B
2.6	Compare and contrast the differences of basic Microsoft Windows OS security settings.		
	User and groups	12.5.1 Users and Groups 12.5.3 User and Group Facts	5A
	Administrator	12.5.1 Users and Groups 12.5.3 User and Group Facts	5A
	Power user	12.5.1 Users and Groups 12.5.3 User and Group Facts	5A

Guest	12.5.1 Users and Groups 12.5.3 User and Group Facts	5A
Standard user	12.5.1 Users and Groups 12.5.3 User and Group Facts	5A
NTFS vs. share permissions		1D, 5B
Allow vs. deny	11.2.3 Attribute Facts 11.3.1 NTFS Permissions 11.3.2 Configure NTFS Permissions 11.3.3 NTFS Permission Facts 11.3.4 Configure NTFS Permissions	5B
Moving vs. copying folders and files	11.2.3 Attribute Facts 11.3.1 NTFS Permissions 11.3.2 Configure NTFS Permissions 11.3.3 NTFS Permission Facts 11.3.4 Configure NTFS Permissions	1D
File attributes	11.2.3 Attribute Facts 11.3.1 NTFS Permissions 11.3.2 Configure NTFS Permissions 11.3.3 NTFS Permission Facts 11.3.4 Configure NTFS Permissions	5B
Shared files and folders		5B
Administrative shares vs. local shares	11.4.1 Shared Folders 11.4.2 Configure Basic Folder Sharing on Windows 11.4.3 Configure Advanced Folder Sharing on Windows 11.4.4 Configure Share and NTFS Permissions 11.4.5 Shared Folder Facts 11.4.6 Share and Secure Folders	5B
Permission propagation	11.4.1 Shared Folders 11.4.2 Configure Basic Folder Sharing on Windows 11.4.3 Configure Advanced Folder Sharing on Windows 11.4.4 Configure Share and NTFS Permissions 11.4.5 Shared Folder Facts 11.4.6 Share and Secure Folders	5B
Inheritance	11.4.1 Shared Folders 11.4.2 Configure Basic Folder Sharing on Windows 11.4.3 Configure Advanced Folder Sharing on Windows 11.4.4 Configure Share and NTFS Permissions 11.4.5 Shared Folder Facts 11.4.6 Share and Secure Folders	5B
System files and folders	11.1.1 System File Locations	1D
User authentication		5A
Single sign-on	13.7.1 Authentication	5A
Run as administrator vs. standard user	12.1.11 Explore System Commands	1C
BitLocker	13.8.5 BitLocker 13.8.6 BitLocker Facts 13.8.7 Use BitLocker	7B
BitLocker To Go	13.8.5 BitLocker 13.8.6 BitLocker Facts 13.8.7 Use BitLocker	7B

	EFS	13.8.1 File Encryption 13.8.2 File Encryption Facts 13.8.3 Encrypt Files 13.8.4 Configure File Encryption	7B
2.7	Given a scenario, implement security best practices to secure a workstation.		
	Password best practices		7A
	Setting strong passwords	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts 13.5.2 Configure BIOS/UEFI Security Settings 13.7.3 Configure Password Policies on Windows	7A
	Password expiration	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts 13.5.2 Configure BIOS/UEFI Security Settings 13.7.3 Configure Password	7A
	Policies on Windows		7A
	Screensaver required password	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts 13.3.5 Configure a Screen Saver Password 13.3.6 Require a Screen Saver Password 13.5.2 Configure BIOS/UEFI Security Settings 13.7.3 Configure Password Policies on Windows	7A
	BIOS/UEFI passwords	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts 13.5.2 Configure BIOS/UEFI Security Settings 13.7.3 Configure Password Policies on Windows	7A
	Requiring passwords	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts 13.5.2 Configure BIOS/UEFI Security Settings 13.7.3 Configure Password Policies on Windows	7A
	Account management	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.1 Users and Groups 12.5.2 Manage Local Users and Groups 12.5.3 User and Group Facts	7A
	Restricting user permissions	12.5.1 Users and Groups	7A
	Logon time restrictions	12.5.3 User and Group Facts	7A
	Disabling guest account	12.5.3 User and Group Facts 13.9.2 Wired Network Security Facts	7A
	Failed attempts lockout	13.7.3 Configure Password Policies on Windows 13.7.4 Password Facts	7A
	Timeout/screen lock	12.1.11 Explore System Commands	7A
	Change default admin user account/password	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts	7A

	Basic Active Directory functions - Account creation	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.2 Manage Local Users and Groups 12.5.3 User and Group Facts	5C
	Basic Active Directory functions - Account deletion	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.3 User and Group Facts	5C
	Basic Active Directory functions - Password reset/unlock account	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 13.7.3 Configure Password Policies on Windows 13.7.4 Password Facts	5C
	Basic Active Directory functions - Disable account	12.4.1 Active Directory Overview 12.4.2 Join a Domain 12.4.3 Join a Workstation to a Domain 12.4.9 Group Policy 12.4.11 Group Policy Facts 12.5.3 User and Group Facts 13.9.2 Wired Network Security Facts	5C
	Disable autorun	13.1.1 Best Practices for Securing Workstations 13.1.2 Workstation Security Facts	6A
	Data encryption	13.8.1 File Encryption 13.8.2 File Encryption Facts 13.8.3 Encrypt Files 13.8.4 Configure File Encrvotion	7B
	Patch/update management	12.10.1 Updates 12.10.3 Update Facts	6A
2.8	Given a scenario, implement methods for securing mobile devices.		
	Screen locks		9A
	Fingerprint lock	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
	Face lock	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
	Swipe lock	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
	Passcode lock	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A

Remote wipes	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Locator applications	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Remote backup applications	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Failed login attempts restrictions	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Antivirus/Anti-malware	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Patching/OS updates	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Biometric authentication	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Full device encryption	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Multifactor authentication	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Authenticator applications	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Trusted sources vs. untrusted sources	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Firewalls	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Policies and procedures		9A
BYOD vs. corporate-owned	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
Profile security requirements	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9A
2.9	Given a scenario, implement appropriate data destruction and disposal methods.	
	Physical destruction	6C
	Shredder	13.3.2 Data Disposal and Destruction 6C
	Drill/hammer	13.3.2 Data Disposal and Destruction 6C
	Electromagnetic (Degaussing)	13.3.2 Data Disposal and Destruction 6C
	Incineration	13.3.2 Data Disposal and Destruction 6C
	Certificate of destruction	13.3.2 Data Disposal and Destruction 6C
	Recycling or repurposing best practices	6C

	Low-level format vs. standard format	13.3.2 Data Disposal and Destruction	6C
	Overwrite	13.3.2 Data Disposal and Destruction	6C
	Drive wipe	13.3.2 Data Disposal and Destruction 13.3.3 Wipe a Disk	6C
2.10	Given a scenario, configure security on SOHO wireless and wired networks.		
	Wireless-specific		4B
	Changing default SSID	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Setting encryption	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Disabling SSID broadcast	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Antenna and access point placement	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Radio power levels	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	WPS	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Change default usernames and passwords	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Enable MAC filtering	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	6A
	Assign static IP addresses		4B
	Firewall settings	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4C
	Port forwarding/mapping	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4C
	Disabling ports	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4C

	Content filtering/parental controls	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4C
	Update firmware	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
	Physical security	13.9.1 Wired Network Security Best Practices 13.9.2 Wired Network Security Facts 13.9.3 Wireless Network Security Best Practices 13.9.4 Wireless Network Security Facts	4B
3.0 Software Troubleshooting			
3.1	Given a scenario, troubleshoot Microsoft Windows OS problems.		
	Common symptoms	7.5.2 Wireless Network Troubleshooting Tool Facts	3C
	Slow performance	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	3C
	Limited connectivity	7.5.1 Wireless Network Troubleshooting 7.5.2 Wireless Network Troubleshooting Tool Facts	4E
	Failure to boot		3C
	No OS found		3C
	Application crashes		3C
	Blue screens		3C
	Black screens	12.14.1 Windows Operating System Issues	3C
	Printing issues	8.6.1 Printer Troubleshooting 8.6.3 Printer Troubleshooting Facts	3C
	Services fail to start	12.1.10 Windows Utilities Facts	3C
	Slow bootup	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	3C
	Slow profile load	12.14.1 Windows Operating System Issues 12.14.2 Troubleshoot Windows Applications 12.14.3 Troubleshoot Windows Services 12.14.4 Application Troubleshooting Facts	3C
	Common solutions	6.10.2 Troubleshoot Network Connectivity 7.5.2 Wireless Network Troubleshooting Tool Facts 10.2.3 Pre-Installation Planning 12.11.1 System Backup 12.11.2 Backup Facts 12.12.1 Windows 10 System Recovery 12.12.10 System Recovery Facts 12.14.5 System Lockups 12.14.6 System Errors Facts 12.15.3 Modify the Boot Order 12.15.5 Using Advanced Boot Options	3C
	Defragment the hard drive		3C
	Reboot	12.15.5 Using Advanced Boot Options	3C
	Kill tasks	12.1.11 Explore System Commands	3C
	Restart services		3C

	Update network settings	6.9 Network Utilities 6.10.2 Troubleshoot Network Connectivity 6.10.3 Network Troubleshooting Facts 6.10.4 Fix a Network Connection 1 7.5.1 Wireless Network Troubleshooting 7.5.2 Wireless Network Troubleshooting Tool Facts	4E
	Reimage/reload OS	13.6.9 Malware Protection Facts	3C
	Roll back updates	4.6.1 Device Driver Troubleshooting	3C
	Roll back devices drivers	4.6.1 Device Driver Troubleshooting	3C
	Apply updates	12.14.5 System Lockups	3C
	Repair application	12.14.6 System Errors Facts	3C
	Update boot order	12.15.3 Modify the Boot Order	3C
	Disable Windows services/applications	12.12.10 System Recovery Facts	3C
	Disable application startup	12.1.10 Windows Utilities Facts	3C
	Safe boot	13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	3C
	Rebuild Windows profiles	10.2.3 Pre-Installation Planning 12.11.1 System Backup 12.11.2 Backup Facts 12.12.1 Windows 10 System Recovery 12.12.10 System Recovery Facts	3C
3.2	Given a scenario, troubleshoot and resolve PC security issues.		
	Common symptoms	12.14.5 System Lockups	8B
	Pop-ups	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Browser redirection	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Security alerts	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Slow performance	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Internet connectivity issues	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	PC/OS lockup	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Application crash	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	OS updates failures	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Rogue antivirus	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B

	Spam	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Renamed system files	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Disappearing files	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	File permission changes	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Hijacked email - Responses from users regarding email	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Hijacked email - Automated replies from unknown sent email	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Access denied	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	Invalid certificate (trusted root CA)	13.13.1 Common Security Issues 13.13.2 Network Security Threat Facts 13.13.3 Security Troubleshooting Facts	8B
	System/application log errors	12.14.5 System Lockups 13.13.1 Common Security Issues 13.13.3 Security Troubleshooting Facts	8B
3.3	Given a scenario, use best practice procedures for malware removal.		
	1. Identify and research malware symptoms.	13.6.3 Malware Protection	8A
	2. Quarantine the infected systems.	13.6.3 Malware Protection	8A
	3. Disable System Restore (in Windows).	13.6.3 Malware Protection	8A
	4. Remediate the infected systems.		8A
	a. Update the anti-malware software.	13.6.3 Malware Protection	8A
	b. Scan and use removal techniques (safe mode, pre-installation environment).	13.6.3 Malware Protection	8A
	5. Schedule scans and run updates.	13.6.3 Malware Protection	8A
	6. Enable System Restore and create a restore point (in Windows).	13.6.3 Malware Protection	8A
	7. Educate the end user.	13.6.3 Malware Protection	8A
3.4	Given a scenario, troubleshoot mobile OS and application issues.		
	Common symptoms		9B
	Dim display	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Intermittent wireless	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	No wireless connectivity	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	No Bluetooth connectivity	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Cannot broadcast to external monitor	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Touchscreen non-responsive	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B

	Apps not loading	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Slow performance	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Unable to decrypt email	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Extremely short battery life		9B
	Overheating	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Frozen system	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	No sound from speakers	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	Inaccurate touch screen response	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	System lockout	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
	App log errors	9.8.1 Mobile Device Troubleshooting 9.8.3 Mobile Device Troubleshooting Facts	9B
3.5	Given a scenario, troubleshoot mobile OS and application security issues.		
	Common symptoms		
	Signal drop/weak signal	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Power drain	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Slow data speeds	9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices 9.8.3 Mobile Device Troubleshooting Facts	9B
	Unintended WiFi connection	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Unintended Bluetooth pairing	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Leaked personal files/data	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Data transmission over limit	9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices 9.8.3 Mobile Device Troubleshooting Facts	9B
	Unauthorized account access	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Unauthorized location tracking	9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B
	Unauthorized camera/microphone activation	9.7.1 Mobile Device Security 9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices	9B

	High resource utilization	9.7.2 Mobile Device Security Facts 9.7.3 Secure Mobile Devices 9.8.3 Mobile Device Troubleshooting Facts	9B
4.0 Operational Procedures			
4.1	Compare and contrast best practices associated with types of documentation.		
	Network topology diagrams	2.6.1 Troubleshooting Process 2.6.2 Troubleshooting Process Facts	10C
	Knowledge base/articles	2.6.1 Troubleshooting Process 2.6.2 Troubleshooting Process Facts	10C
	Incident documentation	13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	10C
	Regulatory and compliance policy	13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts 13.3.7 Physical Security Facts	10C
	Acceptable use policy	13.1.3 Security Policies 13.1.4 Security Policy Facts	10C
	Password policy	13.1.3 Security Policies 13.1.4 Security Policy Facts	10C
	Inventory management		10C
	Asset tags	13.3.7 Physical Security Facts	10C
	Barcodes	4.1.2 Peripheral Device Facts	10C
4.2	Given a scenario, implement basic change management best practices.		
	Documented business processes	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Purpose of the change	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Scope the change	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Risk analysis	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Plan for change	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	End-user acceptance	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Change board		10D
	Approvals	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Backout plan	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
	Document changes	2.3.1 Change Management Overview 2.3.2 Change Management Facts	10D
4.3	Given a scenario, implement basic disaster prevention and recovery methods.		
	Backup and recovery	12.11.1 System Backup 12.11.2 Backup Facts	10E
	Image level	12.11.1 System Backup 12.11.2 Backup Facts	10E
	File level	12.11.1 System Backup 12.11.2 Backup Facts	10E
	Critical applications	12.11.1 System Backup 12.11.2 Backup Facts	10E
	Backup testing	12.11.2 Backup Facts	10E

	UPS	2.5.3 Protect Power 2.5.4 Configure UPS Settings 2.5.5 Power Protection Facts 2.5.6 Install a UPS	10B
	Surge protector	2.5.3 Protect Power 2.5.5 Power Protection Facts	10B
	Cloud storage vs. local storage backups	9.7.2 Mobile Device Security Facts	10E
	Account recovery options	10.2.4 Installation Planning Facts	10E
4.4	Explain common safety procedures.		
	Equipment grounding	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts	10A
	Proper component handling and storage		10A
	Antistatic bags	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts	10A
	ESD straps	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts	10A
	ESD mats	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts	10A
	Self-grounding	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts	10A
	Toxic waste handling		10A
	Batteries	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10A
	Toner	2.1.6 Environmental Concerns	10A
	CRT	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10A
	Cell phones	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10A
	Tablets	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10A
	Personal safety		10A
	Disconnect power before repairing PC	2.1.1 Safety 2.1.2 Safety Measures	10A
	Remove jewelry	2.1.1 Safety 2.1.2 Safety Measures	10A
	Lifting techniques	2.1.1 Safety 2.1.2 Safety Measures	10A
	Weight limitations	2.1.1 Safety 2.1.2 Safety Measures	10A
	Electrical fire safety	2.1.1 Safety 2.1.2 Safety Measures	10A
	Cable management	2.1.1 Safety 2.1.2 Safety Measures	10A
	Safety goggles	2.1.1 Safety 2.1.2 Safety Measures	10A

	Air filter mask	2.1.1 Safety 2.1.2 Safety Measures	10A
	Compliance with government regulations	2.1.1 Safety 2.1.2 Safety Measures	10A
4.5	Explain environmental impacts and appropriate controls.		
	MSDS documentation for handling and disposal	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Temperature, humidity level awareness, and proper ventilation	2.1.3 Electrostatic Discharge 2.1.4 ESD Protection 2.1.5 ESD Facts 2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Power surges, brownouts, and blackouts		10B
	Battery backup	2.5.3 Protect Power 2.5.5 Power Protection Facts	10B
	Surge suppressor	2.5.3 Protect Power 2.5.5 Power Protection Facts	10B
	Protection from airborne particles		10B
	Enclosures	2.1.1 Safety 2.1.2 Safety Measures 2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Air filters/mask	2.1.1 Safety 2.1.2 Safety Measures 2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Dust and debris		10B
	Compressed air	2.1.1 Safety 2.1.2 Safety Measures 2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Vacuums	2.1.1 Safety 2.1.2 Safety Measures 2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
	Compliance to government regulations	2.1.6 Environmental Concerns 2.1.7 Environmental Facts	10B
4.6	Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.		
	Incident response		7C
	First response - Identify	13.2.1 First Responder 13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	7C
	First response - Report through proper channels	13.2.1 First Responder 13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	7C
	First response - Data/device preservation	13.2.1 First Responder 13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	7C

Use of documentation/documentation changes	13.2.1 First Responder 13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	7B
Chain of custody - Tracking of evidence/documenting process	13.2.1 First Responder 13.2.2 Basic Forensic Procedures 13.2.3 Incident Response Facts	7C
Licensing/DRM/EULA	12.9.1 Software Licensing 12.9.2 Digital Rights Management (DRM) 12.9.3 Digital Content Management Facts	7B
Open-source vs. commercial license	12.9.1 Software Licensing 12.9.2 Digital Rights Management (DRM) 12.9.3 Digital Content Management Facts	7B
Personal license vs. enterprise licenses	12.9.1 Software Licensing 12.9.2 Digital Rights Management (DRM) 12.9.3 Digital Content Management Facts	7B
Regulated data		7B
PII	13.4.1 Social Engineering 13.4.2 Social Engineering Facts	7B
PCI	13.4.1 Social Engineering 13.4.2 Social Engineering Facts	7B
GDPR	13.4.1 Social Engineering 13.4.2 Social Engineering Facts	7B
PHI	13.4.1 Social Engineering 13.4.2 Social Engineering Facts	7B
Follow all policies and security best practices	13.1.3 Security Policies 13.1.4 Security Policy Facts	7B
4.7 Given a scenario, use proper communication techniques and professionalism.		
Use proper language and avoid jargon, acronyms, and slang, when applicable	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Maintain a positive attitude/project confidence	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Actively listen (taking notes) and avoid interrupting the customer	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Be culturally sensitive		10G
Use appropriate professional titles, when applicable	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Be on time (if late, contact the customer)	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Avoid distractions		10G
Personal calls	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Texting/social media sites	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Talking to coworkers while interacting with customers	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Personal interruptions	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
Dealing with difficult customers or situations		10G
Do not argue with customers and/or be defensive	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G

	Avoid dismissing customer problems	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Avoid being judgmental	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Do not disclose experiences via social media outlets	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Set and meet expectations/timeline and communicate status with the customer		10G
	Offer different repair/replacement options, if applicable	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Provide proper documentation on the services provided	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Follow up with customer/user at a later date to verify satisfaction	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
	Deal appropriately with customers' confidential and private materials		10G
	Located on a computer, desktop, printer, etc.	2.2.1 Professionalism 2.2.2 Professionalism Facts	10G
4.8	Identify the basics of scripting.		
	Script file types		10F
	.bat	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	.ps1	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	.vbs	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	.sh	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	.py	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	.js	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	Environment variables	1.4.3 Linux Facts 11.1.2 File Location Facts 12.1.7 View System Information 12.14.2 Troubleshoot Windows Applications 13.7.2 Elevate Privileges on Linux	10F
	Comment syntax	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	Basic script constructs	11.2.1 Windows File and Folder Properties	10F
	Basic loops	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	Variables	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	Basic data types		10F
	Integers	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
	Strings	11.2.1 Windows File and Folder Properties 11.2.2 File Extension Facts	10F
4.9	Given a scenario, use remote access technologies.		

RDP	6.5.3 IP Address Facts 6.5.4 TCP/IP Protocol Facts	4D
Telnet	6.5.3 IP Address Facts 6.5.4 TCP/IP Protocol Facts	4D
SSH	6.5.3 IP Address Facts 6.5.4 TCP/IP Protocol Facts	4D
Third-party tools	6.5.3 IP Address Facts 6.5.4 TCP/IP Protocol Facts 12.6.8 Use Screen Sharing 12.6.9 Screen Sharing Facts	4D
Screen share feature	12.6.8 Use Screen Sharing 12.6.9 Screen Sharing Facts	4D
File share	6.5.3 IP Address Facts 6.5.4 TCP/IP Protocol Facts 11.4.5 Shared Folder Facts	4D
Security considerations of each access method	12.6.3 Remote Desktop Facts 12.6.4 Remote Assistance 13.12.1 Virtual Private Networks (VPN)	4D