CompTIA A+ 220-1002
CORRELATION OF STANDARDS WITH

GOODHEART-WILLCOX PUBLISHER
COMPUTER SERVICE AND REPAIR © 2021
BY *RICHARD M. ROBERTS*

Standard	Corresponding Page Number and Heading
1.0 Operating Systems	
1.1 Compare and contrast common operating system types and their purposes.	
32-bit vs. 64-bit	pg. 42 32-Bit and 64-Bit
	pg. 48–62 Microsoft Windows Operating System
	pg. 133–134 32-Bit and 64-Bit Technology
RAM limitations	pg. 63–65 Windows Versions and Editions
	pg. 192 Tech Tip
Software compatibility	pg. 42 32-Bit and 64-Bit
	pg. 72–73 Application Software
	pg. 133–134 32-Bit and 64-Bit Technology
	pg. 134 Software Compatibility
Workstation operating systems	
Microsoft Windows	pg. 48–62 Microsoft Windows Operating System
	pg. 719–729 Microsoft Windows Server
Apple Macintosh OS	pg. 70 Apple Macintosh OS
Linux	pg. 71 Linux
	Appendix C
Cell phone/tablet operating systems	
Microsoft Windows	pg. 70–71 Common Mobile Devices and Operating Systems
	pg. 463 Windows CE
Android	pg. 70–71 Common Mobile Devices and Operating Systems
	pg. 462 Android
iOS	pg. 70 Apple Macintosh OS
	pg. 462 iOS
Chrome OS	pg. 70–71 Common Mobile Devices and Operating Systems
	pg. 463 Chrome OS
Vendor-specific limitations	
End-of-life	pg. 70–71 Tech Tip
	pg. 462 Mobile Operating Systems, second paragraph
Update limitations	pg. 70–71 Tech Tip
	pg. 462–463 Mobile Operating Systems
Compatibility concerns between operating systems	pg. 70–71 Common Mobile Devices and Operating Systems
	pg. 462 Mobile Operating Systems, third paragraph
1.2 Compare and contrast features of Microsoft Windows versions.	
Windows 7	pg. 53–62 Windows Features and Tools
Windows 8	pg. 53–62 Windows Features and Tools
Windows 8.1	pg. 53–62 Windows Features and Tools
Windows 10	pg. 53–62 Windows Features and Tools
Corporate vs. personal needs	pg. 53–62 Windows Features and Tools
Domain access	pg. 718–719 Domain User Account

		pg. 728–729 Joining a Windows Server Domain
	Bitlocker	pg. 55 Drive Encryption
	Media center	pg. 55–56 Desktop Multimedia Support
	Branchcache	pg. 60 BranchCache
	EFS	pg. 342 Encrypted File System
Desktop styles/user interface		pg. 42–45 User Interface
1.3 Summarize general OS installation considerations and upgrade methods.		
Boot methods		pg. 40–41 What Is an Operating System?
	Optical disc (CD-ROM, DVD, Blu-ray)	pg. 40–41 What Is an Operating System?
	External drive	pg. 40–41 What Is an Operating System?
	Network book (PXE)	pg. 40–41 What Is an Operating System?
	Internal fixed disk (HSS/SSD)	pg. 40–41 What Is an Operating System?
	Internal hard drive (partition)	pg. 40–41 What Is an Operating System?
Type of installations		
	Unattended installation	pg. 729–732 Network Unattended Installation
	In-place upgrade	pg. 62–66 Microsoft Windows Installation
	Clean install	pg. 62–66 Microsoft Windows Installation
	Repair installation	pg. 40 Tech Tip
	Multiboot	pg. 69 Dual-Boot and Multiple-Boot Systems
	Remote network installation	pg. 40–41 What Is an Operating System?
	Image deployment	pg. 40–41 What Is an Operating System?
	Recovery partition	pg. 627–628 Windows Recovery Partition
	Refresh/restore	pg. 619–622 Windows 8 Startup Settings
		pg. 623 Windows 10 Startup Settings
Partitioning		pg. 326–340 Disk Partition Systems
	Dynamic	pg. 340 Dynamic Partitioning
	Basic	pg. 339–340 Basic Partitioning
	Primary	pg. 327–330 MBR Partitions
	Extended	pg. 327–330MBR Partitions
	Logical	pg. 340 Logical Partitioning
	GPT	pg. 330–332 GPT Partitions
File system types/formatting		pg. 340–347 File System Formats
	ExFAT	pg. 341 exFAT
	FAT32	pg. 341 FAT16 and FAT32
	NTFS	pg. 341–345 NTFS
	CDFS	pg. 379–380 ISO 9660
	NFS	pg. 345 NFS Formatting
	ext3, ext4	pg. 345–346 Ext3 and Ext4 Formatting
	HFS	pg. 346 HFS Formatting
	Swap partition	pg. 346 Swap Partition
	Quick format vs. full format	pg. 346–347 Formatting a Disk

		pg. 529–530 Disposal of Computer Equipment
	Load alternate third-party drivers when necessary	pg. 109–110 Installing Software Drivers
	Workgroup vs. Domain setup	pg. 694–708 Peer-to-Peer Network Administration pg. 708–719 Centralized Network Administration pg. 698–702 HomeGroup and Libraries pg. 718–719 Domain User Account pg. 728–729 Joining a Windows Server Domain
	Time/date/region/language settings	pg. 54 Data and Time
	Driver installation, software, and Windows updates	pg. 74 Software Patch pg. 109–110 Installing Software Drivers pg. 554–555 Windows Update
	Factory recovery partition	pg. 331 Microsoft Reserved Partition (MSR) pg. 627–628 Windows Recovery Partition
	Properly formatted boot drive with the correct partitions/format	pg. 62–66 Microsoft Windows Installation
	Prerequisites/hardware compatibility	pg. 191–192 Factors to Consider before Upgrading Memory pg. 384 DVD Compatibility Issues pg. 430 Conflicting Devices pg. 605–606 Preparation for Installing or Upgrading an Operating System
	Application compatibility	pg. 42 32-Bit and 64-Bit pg. 72–73 Application Software
	OS compatibility/upgrade path	pg. 62–66 Microsoft Windows installation
1.4 Given a scenario, use appropriate Microsoft command line tools.		
	Navigation	
	dir	pg. 44–45 Command-Line Interface Figure 2-5
	cd	pg. 44–45 Command-Line Interface Figure 2-5
	..	pg. 44–45 Command-Line Interface Figure 2-5
	ipconfig	pg. 744 Running Ipconfig
	ping	pg. 754–755 Ping
	tracert	pg. 755–756 Tracert
	netstat	pg. 757 Netstat
	nslookup	pg. 756 Nslookup
	shutdown	pg. 44–45 Command-Line Interface Figure 2-5
	dism	pg. 44–45 Command-Line Interface Figure 2-5
	sfc	pg. 44–45 Command-Line Interface Figure 2-5

			pg. 592 System File Checker
	chkdsk		pg. 44–45 Command-Line Interface Figure 2-5 pg. 348–350 Chkdsk pg. 608 Chkdsk
	diskpart		pg. 336–337 DiskPart Utility
	taskkill		pg. 44–45 Command-Line Interface Figure 2-5
	gpupdate		pg. 44–45 Command-Line Interface Figure 2-5
	gpresult		pg. 44–45 Command-Line Interface Figure 2-5
	format		pg. 44–45 Command-Line Interface Figure 2-5
	copy		pg. 44–45 Command-Line Interface Figure 2-5
	xcopy		pg. 44–45 Command-Line Interface Figure 2-5
	robocopy		pg. 44–45 Command-Line Interface Figure 2-5
	net use		pg. 717 Net Use Command
	net user		Figure 22-27
	[command name] /?		pg. 44 Tech Tip
	Commands available with standard privileges vs. administrative privileges		pg. 44–45 Command-Line Interface
1.5 Given a scenario, use Microsoft operating system features and tools.			
	Administrative		
		Computer Management	pg. 103–109 System Resources pg. 631 Computer Management
		Device Manager	pg. 103–105 Windows Device Manager
		Local Users and Groups	pg. 535–538 User Accounts
		Local Security Policy	pg. 538–540 Local Security Policy Management
		Performance Monitor	pg. 597–598 Windows Performance, Resource, and Reliability Monitors
		Services	pg. 58 Windows Services Manager pg. 631–633 Task Manager
		System Configuration	pg. 628–629 Microsoft System Configuration Utility
		Task Scheduler	pg. 60 Task Scheduler
		Component Services	pg. 600 Component Services
		Data Sources	pg. 721 Data Sources
		Print Management	pg. 417–418 Print Spooling
		Windows Memory Diagnostics	pg. 599–600 Windows Memory Diagnostics Tools

			pg. 626–627 Windows Recovery Environment
	Windows Firewall		pg. 569–571 Firewall
	Advanced Security		pg. 569–571 Firewall
	Event Viewer		pg. 593–594 Event Viewer
	User Account Management		pg. 535–538 User Accounts
	MSConfig		pg. 628–629 Microsoft System Configuration Utility
		General	pg. 628–629 Microsoft System Configuration Utility Figure 18-10 Figure 18-11 Figure 18-12
		Boot	pg. 628–629 Microsoft System Configuration Utility Figure 18-10 Figure 18-11 Figure 18-12
		Services	pg. 58 Windows Services Manager pg. 628–629 Microsoft System Configuration Utility Figure 18-10 Figure 18-11 Figure 18-12
		Startup	pg. 628–629 Microsoft System Configuration Utility Figure 18-10 Figure 18-11 Figure 18-12
		Tools	pg. 628–629 Microsoft System Configuration Utility Figure 18-10 Figure 18-11 Figure 18-12
	Task Manager		
		Applications	pg. 60 Task Manager pg. 631–633 Task Manager
		Processes	pg. 60 Task Manager pg. 631–633Task Manager
		Performance	pg. 60 Task Manager pg. 631–633Task Manager
		Networking	pg. 60 Task Manager pg. 631–633Task Manager
		Users	pg. 60 Task Manager pg. 631–633Task Manager
	Disk Management		pg. 338 Disk Management
		Drive status	pg. 350 Drive Status
		Mounting	pg. 350 Mounting a Disk pg. 367 Virtual Hard Disk

	Initializing	pg. 333–336 Initializing a Disk
	Extending partitions	pg. 350 Extending Partitions
	Splitting partitions	pg. 351 Splitting Partitions
	Shrink partitions	pg. 351 Shrinking Partitions
	Assigning/changing drive letters	pg. 343–344 Dynamic Disk
	Adding drives	pg. 353–354 PATA Drive Installation
		pg. 351 Adding Drives
	Adding arrays	pg. 344–345 Storage Spaces
	Storage spaces	pg. 344–345Storage Spaces
System utilities		
	Regedit	pg. 48 Configuration Files
	Command	pg. 44–45 Command-Line Interface
	Services.msc	pg. 58 Windows Services Manager
	MMC	pg. 338–339 Disk Management
	MSTSC	pg. 818–820 Remote Desktop
	Notepad	pg. 54 Notepad
	Explorer	pg. 43 Graphical User Interface
	Msinfo32	pg. 630 Microsoft System Information
	DxDiag	pg. 315–316 DirectX Diagnostic Tool
	Disk Defragmenter	pg. 347–348 Disk Defragmenter
	System Restore	pg. 624 System Restore
	Windows Update	pg. 554–555 Windows Update
1.6 Given a scenario, use Microsoft Windows Control Panel utilities.		
Internet Options		
	Connections	pg. 54 Internet Options
	Security	pg. 54 Internet Options
	General	pg. 54 Internet Options
	Privacy	pg. 54 Internet Options
	Programs	pg. 54 Internet Options
	Advanced	pg. 54 Internet Options
Display/Display Settings		
	Resolution	pg. 267–269 Display Resolution
	Color depth	pg. 276–277 Refresh Rate
	Refresh rate	pg. 276–277 Refresh Rate
User Accounts	pg. 535–538 User Accounts	
Folder Options		
	View hidden files	pg. 54 Control Panel
	Hide extensions	pg. 54 Control Panel
	General options	pg. 54 Control Panel
	View options	pg. 54 Control Panel
System		

	Performance (virtual memory)	pg. 54 System
	Remote settings	pg. 54 System
	System protection	pg. 54 System
Windows Firewall		pg. 569–571 Firewall
Power Options		pg. 185–186 Power Management Standards
		pg. 460–462 Windows Power-Management Options
	Hibernate	pg. 461 fourth full paragraph
	Power plans	pg. 185–186 Power Management Standards
		pg. 459–462 Power Management
	Sleep/suspend	pg. 461 third full paragraph
	Standby	pg. 461 third full paragraph
Credential Manager		pg. 576 Determining the Major Fault Area
Programs and features		pg. 576 Determining the Major Fault Area
HomeGroup		pg. 698–702 HomeGroup and Libraries
Devices and Printers		pg. 410–413 Local Printer Installation
Sound		pg. 304–305 Audio Resolution
		pg. 306–307 Speakers
		pg. 308 Sound Cards
Troubleshooting		pg. 596 Windows Problem Reports and Solutions
Network and Sharing Center		pg. 694–695 Network and Sharing Center
Device Manager		pg. 103–105 Windows Device Manager
Bitlocker		pg. 55 Drive Encryption
		pg. 531–532 BitLocker Drive Encryption
Sync Center		pg. 61–62 Sync Your Settings
		pg. 445–447 Synchronization
1.7 Summarize application installation and configuration concepts.		
System requirements		pg. 63–65 Windows Versions and Editions
	Drive space	pg. 63–65 Windows Versions and Editions
	RAM	pg. 63–65 Windows Versions and Editions
OS requirements		pg. 63–65 Windows Versions and Editions
	Compatibility	pg. 63–65 Windows Versions and Editions
Methods of installation and deployment		
	Local (CD/USB)	pg. 40–41 What Is an Operating System?
	Network-based	pg. 40–41 What Is an Operating System?
		pg. 629–632 Network Unattended Installation
Local user permissions		pg. 535–538 User Accounts
		pg. 725–727 Permissions
	Folder/file access for installation	pg. 714 Administrator vs. Standard User
Security considerations		
	Impact to device	pg. 538–540 Local Security Policy Management
	Impact to network	pg. 538–540 Local Security Policy Management

1.8 Given a scenario, configure Microsoft Windows networking on a client/desktop.		
	HomeGroup vs. Workgroup	pg. 694–708 Peer-to-Peer Network Administration
		pg. 708–719 Centralized Network Administration
		pg. 698–702 HomeGroup and Libraries
	Domain setup	pg. 715–716 Network Administration Models
		pg. 698–702 HomeGroup and Libraries
	Network shares/administrative shares/mapping drives	pg. 694–695 Network and Sharing Center pg. pg. 700–701 Password-Protected Sharing
		pg. 702–704 Advanced File Sharing
		pg. 701–702 Network Discovery
	Printer sharing vs. network printer mapping	pg. 416–417 Sharing Printers
	Establish networking connections	pg. 701–702 Network Discovery
	VPN	pg. 801–802 Virtual Private Network (VPN)
	Dial-ups	pg. 498–499 Telephone Modem Installation
	Wireless	pg. 463–467 Wireless Connections
	Wired	pg. 810–811 Configure a New Network Connection
	WWAN (Cellular)	pg. 642 Tech Tip (top)
	Proxy settings	pg. 751 Proxy Server
	Remote Desktop Connection	pg. 818–820 Remote Desktop
	Remote Assistance	pg. 595–596 Remote Assistance
	Home vs. Work vs. Public network settings	pg. 701–702 Network Discovery
	Firewall settings	
	Exceptions	pg. 569–571 Firewall
	Configuration	pg. 569–571 Firewall
		pg. 800–801 Firewall
	Enabling/disabling Windows Firewall	pg. 569–571 Firewall
	Configuring an alternative IP address in Windows	pg. 745–746 Alternate IP Address
	IP addressing	pg. 740–741 IP Addresses
	Subnet mask	pg. 743. IPv4 Subnet Mask
	DNS	pg. 747 DNS
	Gateway	pg. 751 Gateway
	Network card properties	pg. 645–647 Network Interface Cards
	Half duplex/full duplex/auto	pg. 656–657 Network Adapter Speed and Operation Mode
	Speed	pg. 655–657 Installing a Typical Network Interface Card
	Wake-on-LAN	pg. 656 Wake-on-LAN
	QoS	pg. 673–674 VoIP
		pg. 673 Tech Tip
		pg. 742 Better Quality of Service
	BIOS (on-board NIC)	pg. 67 BIOS
1.9 Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems.		
	Best practices	
	Scheduled backups	Appendix C Scheduled Backups

	Scheduled disk maintenance	Appendix C Scheduled Disk Maintenance
	System updates/App Store	Appendix C System Updates and App Store
	Patch management	Appendix C Patch, Driver, and Firmware Management
	Driver/firmware updates	Appendix C Patch, Driver, and Firmware Management
	Antivirus/Anti-malware updates	Appendix C Antivirus and Antimalware Updates
Tools		
	Backup/Time Machine	Appendix C Scheduled Backups
	Restore/Snapshot	Appendix C Scheduled Backups
	Image recovery	Appendix C Scheduled Backups
	Disk maintenance utilities	Appendix C Scheduled Disk Maintenance
	Shell/Terminal	Appendix C Scheduled Disk Maintenance
	Screen sharing	Appendix C Sharing Screens and Files
	Force Quit	Appendix C Macintosh Tools and Features
Features		
	Multiple desktops/Mission Control	Appendix C Sharing Screens and Files
	Key Chain	Appendix C Cross-Platform Tools and Features
	Spot Light	Appendix C Searching with Spotlight
	iCloud	Appendix C Cross-Platform Tools and Features
	Gestures	Appendix C Cross-Platform Tools and Features
	Finder	Appendix C Searching with Spotlight
	Remote Disc	Appendix C Sharing Screens and Files
	Dock	Appendix C Cross-Platform Tools and Features
	Boot Camp	Appendix C Installing Windows Operating System via Boot Camp
Basic Linux commands		
	ls	Appendix B Linux Shell Commands
	grep	Appendix B Linux Shell Commands
	cd	Appendix B Linux Shell Commands
	shutdown	Appendix B Linux Shell Commands
	pwd vs. passwd	Appendix B Linux Shell Commands
	mv	Appendix B Linux Shell Commands
	cp	Appendix B Linux Shell Commands
	rm	Appendix B Linux Shell Commands
	chmod	Appendix B Linux Shell Commands
	chown	Appendix B Linux Shell Commands
	iwconfig/ifconfig	Appendix B Linux Shell Commands
	ps	Appendix B Linux Shell Commands
	su/sudo	Appendix B Linux Shell Commands
	apt-get	Appendix B Linux Shell Commands
	vi	Appendix B Linux Shell Commands
	dd	Appendix B Linux Shell Commands

	kill	Appendix B Linux Shell Commands
2.0 Security		
	2.1 Summarize the importance of physical security measures.	
	Mantrap	pg. 525 Physical Security
	Badge reader	pg. 526–528 Radio-Frequency Identification
	Smart card	pg. 528–529 Smart Cards and Virtual Smart Cards
	Security guard	pg. 525 Physical Security
	Door lock	pg. 526 Securing the Physical Area
	Biometric locks	pg. 469 Smart Cards and Biometrics pg. 472–473 Face Lock pg. 534 Multifactor Authentication
	Hardware tokens	pg. 528 Tech Tip
	Cable locks	pg. 474 Physical Locks
	Server locks	pg. 526 Securing the Physical Area
	USB locks	pg. 526 Securing the Physical Area
	Privacy screen	pg. 529 Privacy Filter
	Key fobs	pg. 526–528 Radio-Frequency Identification
	Entry control roster	pg. 525 Physical Security
	2.2 Explain logical security concepts.	
	Active Directory	pg. 709–710 Microsoft Windows Server
	Login script	pg. 725 Login Scripts
	Domain	pg. 715–716 Domains
	Group Policy/Updates	pg. 541 Local Group Policy Management
	Organizational Units	pg. 717–718 Default Users and Groups
	Home Folder	pg. 728 Folder Redirection
	Folder redirection	pg. 728 Folder Redirection
	Software tokens	pg. 528 Tech Tip
	MDM policies	pg. 716 MDM Policies
	Port security	pg. 800–801 Firewall
	MAC address filtering	pg. 803 Enable MAC Filtering
	Certificates	pg. 532 Tech Tip
	Antivirus/Anti-malware	pg. 551 Microsoft Malicious Software Removal Tool pg. 565–566 Malware Prevention
	Firewalls	pg. 569–571 Firewall
	User authentication/strong passwords	pg. 532–534 Passwords pg. 721–723 Password Policy
	Multifactor authentication	pg. 534–535 Multifactor Authentication
	Directory permissions	pg. 704–705 Share Permissions and Security Permissions
	VPN	pg. 801–802 Virtual Private Network (VPN)
	DLP	pg. 541 User Security Education
	Access control lists	pg. 704–705 Share Permissions and Security Permissions

	Smart card	pg. 528–529 Smart Cards and Virtual Smart Cards
	Email filtering	pg. 535–538 User Accounts
	Trusted/untrusted software sources	pg. 565–566 Malware Prevention
		pg. 549–550 Trusted Boot and Measured Boot Security
	Principle of least privilege	pg. 538 Principle of Least Privilege
2.3 Compare and contrast wireless security protocols and authentication methods.		
	Protocols and encryption	
	WEP	pg. 470 Wireless Network Security and Encryption Types
	WPA	pg. 471 first paragraph
	WPA2	pg. 471 first paragraph
	TKIP	pg. 471 second paragraph
	AES	pg. 471 second paragraph
	Authentication	pg. 532–538 Authentication and Education
	Single-factor	pg. 532–534 Passwords
	Multifactor	pg. 534–535 Multifactor Authentication
	RADIUS	pg. 532 Authentication and Education
		pg. 714 RADIUS
	TACACS	pg. 532 Authentication and Education
		pg. 714–715 TACACS
2.4 Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.		
	Malware	pg. 556–564 Malicious Software
	Ransomware	pg. 562 Ransomware
	Trojan	pg. 557 Trojan Horse
	Keylogger	pg. 558–559 Password Virus
	Rootkit	pg. 560 Rootkit
	Virus	pg. 556 Malicious Software
	Botnet	pg. 560 Botnet
	Worm	pg. 5567–557 Worm
	Spyware	pg. 561 Spyware
		pg. 560–561 Adware
	Tools and methods	
	Antivirus	pg. 551 Microsoft Malicious Software Removal Tool
		pg. 565–566 Malware Prevention
	Anti-malware	pg. 551 Microsoft Malicious Software Removal Tool
		pg. 565–566 Malware Prevention
	Recovery console	pg. 624–626 Recovery Console
	Backup/restore	pg. 624 System Restore
		pg. 606 System Backups
	End user education	pg. 541 User Security Education
	Software firewalls	pg. 569–571 Firewall
	SecureDNS	pg. 532 Authentication and Education

2.5 Compare and contrast social engineering, threats, and vulnerabilities.		
Social engineering		pg. 541 Social Engineering
	Phishing	pg. 562 Phishing
	Spear phishing	pg. 562 Phishing
	Impersonation	pg. 541 Social Engineering
	Shoulder surfing	pg. 529 Privacy Filters
	Tailgating	pg. 525 Physical Security
	Dumpster diving	pg. 529 Dumpster Diving
DDoS		pg. 560 Botnet
DoS		pg. 560 Botnet
Zero-day		pg. 566 Tech Tip
Man-in-the-middle		pg. 563–564 Man-in-the-Middle (MITM)
Brute force		pg. 533 Protecting Your Passwords
Dictionary		pg. 533 Protecting Your Passwords
		pg. 723 Account Lockout Policy
Rainbow table		pg. 533 Protecting Your Passwords
Spoofing		pg. 535–538 User Accounts
Non-compliant systems		pg. 565–566 Malware Prevention
Zombie		pg. 561–562 Spam
2.6 Compare and contrast the differences of basic Microsoft Windows OS security settings.		
User and groups		pg. 716 Groups
		pg. 716 Users
		pg. 717–718 Default Users and Groups
	Administrator	pg. 716–717 System Administrator
		pg. 714 Administrator vs. Standard User
	Power user	pg. 705 Local Power Users
	Guest	pg. 535–538 User Accounts
		pg. 717–718 Default Users and Groups
	Standard user	pg. 716 Users
		pg. 717–718 Default Users and Groups
		pg. 719–718 Domain User Account
		pg. 714 Administrator vs. Standard User
NTFS vs. share permissions		pg. 704–705 Share Permissions and Security Permissions
	Allow vs. deny	pg. 705 Allow vs. Deny Share Permissions
	Moving vs. copying folders and files	pg. 706 Moving and Copying Folders and Files
	File attributes	pg. 706 File Attributes
Shared files and folders		pg. 694–695 Network and Sharing Center
		pg. 700–701 Password-Protected Sharing
		pg. 702–704 Advanced File Sharing
		pg. 814–815 Share Files and Folders in Windows
	Administrative shares vs. local shares	pg. 707–708 Administrative Shares vs. Local Shares
	Permission propagation	pg. 708 Permission Propagation

			Inheritance	pg. 708 Permission Propagation
		System files and folders		pg. 46–47 File System Structure
				pg. 47 File Systems
				pg. 47–48 Configuration Files
				pg. 340–347 File System Formats
		User authentication		pg. 532–541 Authentication and Education
			Single sign-on	pg. 718–719 Domain User Account
		Run as administrator vs. standard user		pg. 714 Administrator vs. Standard User
		BitLocker		pg. 55 Drive Encryption
				pg. 531–532 BitLocker Drive Encryption
		BitLocker To Go		pg. 55 Drive Encryption
				pg. 531–532 BitLocker Drive Encryption
		EFS		pg. 342 Encrypted File System
	2.7 Given a scenario, implement security best practices to secure a workstation.			
		Password best practices		pg. 532–534 Passwords
				pg. 721–723 Password Policy
			Setting strong passwords	pg. 532–534 Passwords
				pg. 721–723 Password Policy
			Password expiration	pg. 721–723 Password Policy
			Screensaver required password	pg. 534 Screen Saver Password
			BIOS/UEFI passwords	pg. 533–534 System Configuration Passwords
			Requiring passwords	pg. 532–534 Passwords
				pg. 721–723 Password Policy
		Account management		
			Restricting user permissions	pg. 535–538 User Accounts
			Logon time restrictions	pg. 724 Time Policy
			Disabling guest account	pg. 535–538User Accounts
			Failed attempts lockout	pg. 723 Account Lockout Policy
			Timeout/screen lock	pg. 534 Screen Saver Password
			Change default admin user account/password	pg. 717 Creating Passwords
				pg. 803 Change Default Names
			Basic Active Directory functions	
			Account creation	pg. 716–717 System Administrator
			Account deletion	pg. 720–721 User Management
			Password reset/unlock account	pg. 720–721User Management
			Disable account	pg. 720–721User Management
		Disable autorun		pg. 395 Failure to AutoPlay Disc
		Data encryption		pg. 470–471 Wireless Network Security and Encryption Types
		Patch/update management		pg. 74 Software Patch
				pg. 554–555 Windows Update
	2.8 Given a scenario, implement methods for securing mobile devices.			
		Screen locks		

		Fingerprint lock	pg. 534–535 Multifactor Authentication
		Face lock	pg. 472–473 Face Lock
		Swipe lock	pg. 473 Swipe Lock
		Passcode lock	pg. 472 Passcode Lock
	Remote wipes		pg. 474 Company Apps
	Locator applications		pg. 442 Global Positioning System
	Remote backup applications		pg. 443 Cloud Services
	Failed login attempts restrictions		pg. 473 Device Access Failure pg. 723 Account Lockout Policy
	Antivirus/Anti-malware		pg. 551 Microsoft Malicious Software Removal Tool pg. 565–566 Malware Prevention
	Patching/OS updates		pg. 74 Software Patch pg. 554–555 Windows Update
	Biometric authentication		pg. 534–535 Multifactor Authentication
	Full device encryption		pg. 55 Drive Encryption pg. 531–532 BitLocker Drive Encryption
	Multifactor authentication		pg. 534–535 Multifactor Authentication
	Authenticator applications		pg. 531–532 BitLocker Drive Encryption
	Trusted sources vs. untrusted sources		pg. 565–566 Malware Prevention pg. 549–550 Trusted Boot and Measured Boot Security
	Firewalls		pg. 569–571 Firewall
	Policies and procedures		
		BYOD vs. corporate-owned	pg. 808–809 Using Policies to Harden Security
		Profile security requirements	pg. 808–809 Using Policies to Harden Security
2.9 Given a scenario, implement appropriate data destruction and disposal methods.			
	Physical destruction		pg. 529–530 Disposal of Computer Equipment
		Shredder	pg. 529–530 Disposal of Computer Equipment
		Drill/hammer	pg. 529–530 Disposal of Computer Equipment
		Electromagnetic (Degaussing)	pg. 529–530 Disposal of Computer Equipment
		Incineration	pg. 529–530 Disposal of Computer Equipment
		Certificate of destruction	pg. 529–530 Disposal of Computer Equipment
	Recycling or repurposing best practices		pg. 529–530 Disposal of Computer Equipment
		Low-level format vs. standard format	pg. 346–347 Formatting a Disk pg. 529–530 Disposal of Computer Equipment
		Overwrite	pg. 529–530 Disposal of Computer Equipment
		Drive wipe	pg. 529–530 Disposal of Computer Equipment
2.10 Given a scenario, configure security on SOHO wireless and wired networks.			
	Wireless-specific		
		Changing default SSID	pg. 803 Change Default Names
		Setting encryption	pg. 790–791 Wireless pg. 803 Change Default Names

		Disabling SSID broadcast	pg. 804 Disable SSID Broadcast
		Antenna and access point placement	pg. 795 Data Transfer Rates pg. 797–799 Internet Access and SOHO Design
		Radio power levels	pg. 650–652 Wireless Routers
		WPS	pg. 651–652 WPS
	Change default usernames and passwords		pg. 803 Change Default Names
	Enable MAC filtering		pg. 803 Enable MAC Filtering
	Assign static IP addresses		pg. 745 DHCP pg. 805 Port Forwarding pg. 806 Single Port Forwarding
	Firewall settings		pg. 569–571 Firewall pg. 751–753 Firewall
	Port forwarding/mapping		pg. 805 Port Forwarding pg. 806 Single Port Forwarding
	Disabling ports		pg. 569–571 Firewall pg. 751–753 Firewall pg. 800–801 Firewall
	Content filtering/parental controls		pg. 548–549 Parental Controls and Family Options
	Update firmware		pg. 394 Firmware Update
	Physical security		pg. 525–532 Physical Security
3.0 Software Troubleshooting			
	3.1 Given a scenario, troubleshoot Microsoft Windows OS problems.		
	Common symptoms		
		Slow performance	pg. 484 Symptom 20 pg. 588–589 Read and Write Failure
		Limited connectivity	pg. 782 Limited Connectivity
		Failure to boot	pg. 583 Symptom 2 pg. 583 Symptom 3 pg. 583 Symptom 4
		No OS found	pg. 580 Second Stage pg. 583 Symptom 2 pg. 583 Symptom 3 pg. 583 Symptom 4
		Application crashes	pg. 585 Symptom 9
		Blue screens	pg. 481 Symptom 6 pg. 582 Blue Screen Error pg. 583 Symptom 4
		Black screens	pg. 480 Symptom 2 pg. 583 Symptom 2 pg. 583 Symptom 3
		Printing issues	pg. 418–432 Troubleshooting Printers
		Services fail to start	pg. 586 Symptom 11

		Slow bootup	pg. 481 Symptom 5
		Slow profile load	pg. 586 Symptom 12
	Common solutions		
		Defragment the hard drive	pg. 347–348 Disk Defragmenter
		Reboot	pg. 578–580 First Stage
		Kill tasks	pg. 631–633 Task Manager
		Restart services	pg. 631–633 Task Manager
		Update network settings	pg. 576 Determining the Major Fault Area
		Reimage/reload OS	pg. 633 Reinstall the Operating System
		Roll back updates	pg. 612 Verify Full System Functionality and Implement Preventive Measures
		Roll back devices drivers	pg. 624 Tech Tip
		Apply updates	pg. 554–555 Windows Update
		Repair application	pg. 631–633Task Manager
		Update boot order	pg. 584 Symptom 7
		Disable Windows services/applications	pg. 628–629 Microsoft System Configuration Utility
		Disable application startup	pg. 628–629 Microsoft System Configuration Utility
		Safe boot	pg. 617–619 Advanced Boot Options
		Rebuild Windows profiles	pg. 586 Symptom 12
	3.2 Given a scenario, troubleshoot and resolve PC security issues.		
	Common symptoms		
		Pop-ups	Figure 16-12
		Browser redirection	Figure 16-12
		Security alerts	Figure 16-12
		Slow performance	pg. 481 Symptom 3 Figure 16-12 pg. 588–589 Read and Write Failure
		Internet connectivity issues	Figure 16-12 pg. 482 Symptom 13 pg. 483 Symptom 15
		PC/OS lockup	Figure 16-12 pg. 484 Symptom 24 pg. 485 Symptom 28 pg. 590 System Lockups
		Application crash	pg. 585 Symptom 9
		OS updates failures	Figure 16-12
		Rogue antivirus	Figure 16-12
		Spam	pg. 561–562 Spam Figure 16-12
		Renamed system files	Figure 16-12
		Disappearing files	Figure 16-12
		File permission changes	Figure 16-12

	Hijacked email	Figure 16-12
		pg. 713 Hijacked E-Mail
	Responses from users regarding email	pg. 713Hijacked E-Mail
	Automated replies from unknown sent email	pg. 713Hijacked E-Mail
	Access denied	pg. 591 Mobile OS and Application Issues
	Invalid certificate (trusted root CA)	pg. 532 Tech Tip
		Figure 16-12
	System/application log errors	Figure 16-12
3.3 Given a scenario, use best practice procedures for malware removal.		
	1. Identify and research malware symptoms.	pg. 566–567 Malware Removal
	2. Quarantine the infected systems.	pg. 566–567 Malware Removal
	3. Disable System Restore (in Windows).	pg. 566–567 Malware Removal
	4. Remediate the infected systems.	pg. 566–567 Malware Removal
	a. Update the anti-malware software.	pg. 566–567 Malware Removal
	b. Scan and use removal techniques (safe mode, pre-installation environment).	pg. 566–567 Malware Removal
	5. Schedule scans and run updates.	pg. 566–567 Malware Removal
	6. Enable System Restore and create a restore point (in Windows).	pg. 566–567 Malware Removal
	7. Educate the end user.	pg. 566–567 Malware Removal
3.4 Given a scenario, troubleshoot mobile OS and application issues.		
	Common symptoms	
	Dim display	pg. 482 Symptom 11
	Intermittent wireless	pg. 784 Intermittent Connectivity
	No wireless connectivity	pg. 483 Symptom 15
		pg. 782 No Wireless via Mobile Devices
	No Bluetooth connectivity	pg. 483 Symptom 16
		pg. 782 No Wireless via Mobile Devices
	Cannot broadcast to external monitor	pg. 483 Symptom 17
	Touchscreen non-responsive	pg. 483 Symptom 18
	Apps not loading	pg. 483 Symptom 19
	Slow performance	pg. 484 Symptom 20
	Unable to decrypt email	pg. 483 Symptom 21
		pg. 714 E-Mail Decryption Errors
	Extremely short battery life	pg. 484 Symptom 22
	Overheating	pg. 484 Symptom 23
		pg. 590–591 Intermittent Device Failures
	Frozen system	pg. 484 Symptom 24
	No sound from speakers	pg. 306–307 Speakers
		pg. 485 Symptom 25
	Inaccurate touch screen response	pg. 483 Symptom 18
	System lockout	pg. 484 Symptom 24

		pg. 485 Symptom 28
		pg. 590 System Lockups
	App log errors	pg. 591 Mobile OS and Application Issues
3.5 Given a scenario, troubleshoot mobile OS and application security issues.		
	Common symptoms	
	Signal drop/weak signal	pg. 485 Symptom 29
	Power drain	pg. 486 Symptom 30
	Slow data speeds	pg. 486 Symptom 31
	Unintended WiFi connection	pg. 486 Symptom 32
	Unintended Bluetooth pairing	pg. 486 Symptom 33
	Leaked personal files/data	pg. 486 Symptom 34
	Data transmission over limit	pg. 486 Symptom 35
	Unauthorized account access	pg. 487 Symptom 36
	Unauthorized location tracking	pg. 487 Symptom 37
	Unauthorized camera/microphone activation	pg. 487 Symptom 38
	High resource utilization	pg. 487 Symptom 39
4.0 Operational Procedures		
	4.1 Compare and contrast best practices associated with types of documentation.	
	Network topology diagrams	pg. 642–645 Network Topologies
		Figure 19-3
		Figure 19-4
		Figure 19-5
		Figure 19-6
	Knowledge base/articles	pg. 832 Knowledge Base and Articles
	Incident documentation	pg. 832 Incident Documentation
	Regulatory and compliance policy	pg. 832 Regulatory and Compliance Policy
	Acceptable use policy	pg. 832 Acceptable Use Policy
	Password policy	pg. 532–534 Passwords
		pg. 565–566 Malware Prevention
		pg. 721–723 Password Policy
	Inventory management	
	Asset tags	pg. 833 Inventory Management
	Barcodes	pg. 833 Inventory Management
	4.2 Given a scenario, implement basic change management best practices.	
	Documented business processes	pg. 833 Documented Business Processes
	Purpose of the change	pg. 833 Purpose of the Change
	Scope the change	pg. 834 Scope of the Change
	Risk analysis	pg. 834 Risk Analysis
	Plan for change	pg. 834 Plan for Change
	End-user acceptance	pg. 834 End-User Acceptance
	Change board	pg. 834 Change Board

	Approvals	pg. 834 Change Board
	Backout plan	pg. 834–835 Backout Plan
	Document changes	pg. 835 Document Changes
4.3 Given a scenario, implement basic disaster prevention and recovery methods.		
	Backup and recovery	pg. 606 System Backups pg. 624–626 Recovery Console pg. 626–627 Windows Recovery Environment
	Image level	pg. 606–607 System Image
	File level	pg. 633–634 Data Recovery Techniques
	Critical applications	pg. 633–634 Data Recovery Techniques
	Backup testing	pg. 633–634 Data Recovery Techniques
	UPS	pg. 181–182 UPS Systems
	Surge protector	pg. 180–183 Surge-Protection Devices pg. 182–183 Power Strips
	Cloud storage vs. local storage backups	pg. 633–634 Data Recovery Techniques
	Account recovery options	pg. 633–634 Data Recovery Techniques
4.4 Explain common safety procedures.		
	Equipment grounding	pg. 170 Grounding
	Proper component handling and storage	pg. 28–29 Electrostatic Discharge (ESD)
	Antistatic bags	Figure 1-34
	ESD straps	Figure 1-32
	ESD mats	Figure 1-33
	Self-grounding	pg. 28 Tech Tip
	Toxic waste handling	
	Batteries	pg. 449–450 Batteries
	Toner	pg. 430–431 Toner Spills
	CRT	pg. 269 Caution
	Cell phones	pg. 440 Caution!
	Tablets	pg. 440 Caution!
	Personal safety	
	Disconnect power before repairing PC	pg. 33 Electrical Safety
	Remove jewelry	pg. 33 Electrical Safety
	Lifting techniques	pg. 31–32 Physical Safety
	Weight limitations	pg. 31–32 Physical Safety
	Electrical fire safety	pg. 33–34 Fire Safety
	Cable management	pg. 31–32 Physical Safety
	Safety goggles	pg. 31–32 Physical Safety
	Air filter mask	pg. 31–32 Physical Safety
	Compliance with government regulations	pg. 34–35 Chemical Safety pg. 184 Battery Disposal pg. 449–450 Batteries

4.5 Explain environmental impacts and appropriate controls.		
	MSDS documentation for handling and disposal	pg. 34–35 Chemical Safety pg. 184 Battery Disposal pg. 430–431 Toner Spills
	Temperature, humidity level awareness, and proper ventilation	pg. 282 Cleaning Video Displays
	Power surges, brownouts, and blackouts	pg. 180–183 Surge-Protection Devices
	Battery backup	pg. 180–183 Surge-Protection Devices
	Surge suppressor	pg. 180–183 Surge-Protection Devices
	Protection from airborne particles	pg. 32–33 Physical Safety
	Enclosures	pg. 32–33 Physical Safety
	Air filters/mask	pg. 32–33 Physical Safety
	Dust and debris	
	Compressed air	pg. 30–31 Tool Kit
	Vacuums	pg. 430–431 Toner Spills
	Compliance to government regulations	pg. 34–35 Chemical Safety pg. 184 Battery Disposal pg. 449–450 Batteries
4.6 Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.		
	Incident response	
	First response	pg. 848 First Response/Incident Response
	Identify	pg. 848 Identify
	Report through proper channels	pg. 848 Report through Proper Channels
	Data/device preservation	pg. 848 Preserving Data and Devices
	Use of documentation/documentation changes	pg. 849 Documentation
	Chain of custody	pg. 849 Chain of Custody
	Tracking of evidence/documenting process	pg. 849 Chain of Custody
	Licensing/DRM/EULA	pg. 388–390 Digital Rights Management
	Open-source vs. commercial license	pg. 388 Digital Rights Management
	Personal license vs. enterprise licenses	pg. 388 Tech Tip (bottom)
	Regulated data	
	PII	pg. 842–843 Customer's Confidential Materials
	PCI	pg. 842–843 Customer's Confidential Materials
	GDPR	pg. 842–843 Customer's Confidential Materials
	PHI	pg. 842–843 Customer's Confidential Materials
	Follow all policies and security best practices	pg. 541 User Security Education pg. 846–850 Dealing With Prohibited Content or Activity
4.7 Given a scenario, use proper communication techniques and professionalism.		
	Use proper language and avoid jargon, acronyms, and slang, when applicable	pg. 835–836 Verbal Communication
	Maintain a positive attitude/project confidence	pg. 836–837 Attitude

	Actively listen (taking notes) and avoid interrupting the customer	pg. 838 Listening Skills
	Be culturally sensitive	pg. 837 Be Culturally Sensitive
	Use appropriate professional titles, when applicable	pg. 837 Be Culturally Sensitive
	Be on time (if late, contact the customer)	pg. 837 Be on Time
	Avoid distractions	pg. 838 Avoid Distractions
	Personal calls	pg. 838 Avoid Distractions
	Texting/social media sites	pg. 838 Avoid Distractions
	Talking to coworkers while interacting with customers	pg. 838 Avoid Distractions
	Personal interruptions	pg. 838 Avoid Distractions
	Dealing with difficult customers or situations	pg. 843–844 Handling Difficult Situations
	Do not argue with customers and/or be defensive	pg. 843–844 Handling Difficult Situations pg. 844 Is the Customer Always Right?
	Avoid dismissing customer problems	pg. 843–844 Handling Difficult Situations
	Avoid being judgmental	pg. 836–837 Attitude
	Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)	pg. 838 Listening Skills
	Do not disclose experiences via social media outlets	pg. 842–843 Customer's Confidential Materials
	Set and meet expectations/timeline and communicate status with the customer	pg. 844 Your Word
	Offer different repair/replacement options, if applicable	pg. 843–844 Handling Difficult Situations pg. 844 Your Word
	Provide proper documentation on the services provided	pg. 844–845 Contracts
	Follow up with customer/user at a later date to verify satisfaction	pg. 844 Follow-Up
	Deal appropriately with customers' confidential and private materials	pg. 842–843 Customer's Confidential Materials
	Located on a computer, desktop, printer, etc.	pg. 842–843 Customer's Confidential Materials
4.8 Identify the basics of scripting.		
	Script file types	Appendix B Figure B-1
	.bat	Appendix B Figure B-1
	.ps1	Appendix B Figure B-1
	.vbs	Appendix B Figure B-1

		.sh	Appendix B Figure B-1
		.py	Appendix B Figure B-1
		.js	Appendix B Figure B-1
	Environment variables		Appendix B
	Comment syntax		Appendix B
	Basic script constructs		Appendix B
		Basic loops	Appendix B Figure B-2
		Variables	Appendix B Figure B-2
	Basic data types		Appendix B
		Integers	Appendix B Figure B-3
		Strings	Appendix B Figure B-3
4.9 Given a scenario, use remote access technologies.			
	RDP		pg. 818–820 Remote Desktop Figure 23-33 Figure 23-34
	Telnet		pg. 771 Telnet Figure 22-13
	SSH		pg. 770–771 SSH
	Third-party tools		
		Screen share failure	pg. 778 Other Cloud-Computing Tools
		File share	pg. 778 Other Cloud-Computing Tools
	Security considerations of each access method		pg. 778 Other Cloud-Computing Tools