CompTIA A+ Core 2 (220-1102)

1.0 Operating System

1.1 Identify basic features of Microsoft Windows editions.

Objectives	Primary Module
• Windows 10 editions	Installing Windows
• Home	Installing Windows
• Pro	Installing Windows
• Pro for Workstations	Installing Windows
• Enterprise	Installing Windows
• Feature differences	Installing Windows
• Domain access vs. workgroup	Installing Windows

Objectives	Primary Module
• Desktop styles/user interface	Installing Windows
• Availability of Remote Desktop Protocol (RDP)	Installing Windows
• Random-access memory (RAM) support limitations	Installing Windows
• BitLocker	Installing Windows
• gpedit.msc	Installing Windows
• Upgrade paths	The Complex World of IT Professionals
• In-place upgrade	The Complex World of IT Professionals

1.2 Given a scenario, use the appropriate Microsoft command-line tool.

Objectives	Primary Module
• Navigation	Maintaining Windows

Objectives	Primary Module
• cd	Maintaining Windows
• dir	Maintaining Windows
• md	Maintaining Windows
• rmdir	Maintaining Windows
• Drive navigation inputs:	Maintaining Windows
• C:\ or D:\ or x:\	Maintaining Windows
• Command-line tools	
• ipconfig	Network Security and Troubleshooting
• ping	Network Security and Troubleshooting
• hostname	Network Security and Troubleshooting
• netstat	Network Security and Troubleshooting

Objectives	Primary Module
• nslookup	Network Security and Troubleshooting
• chkdsk	Maintaining Windows
• net user	Network Security and Troubleshooting
• net use	Network Security and Troubleshooting
• tracert	Network Security and Troubleshooting
• format	Maintaining Windows
• xcopy	Maintaining Windows
• copy	Maintaining Windows
• robocopy	Maintaining Windows
• gpupdate	Securing and Sharing Windows Resources
• gpresult	Securing and Sharing Windows Resources

Objectives	Primary Module
• shutdown	Maintaining Windows
• sfc	Troubleshooting Windows After Startup
• [command name] /?	Maintaining Windows
• diskpart	Maintaining Windows
• pathping	Network Security and Troubleshooting
• winver	Maintaining Windows

1.3 Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

Objectives	Primary Module
• Task Manager	Troubleshooting Windows After Startup
• Services	Troubleshooting Windows After Startup

Objectives	Primary Module
• Startup	Troubleshooting Windows After Startup
• Performance	Troubleshooting Windows After Startup
• Processes	Troubleshooting Windows After Startup
• Users	Troubleshooting Windows After Startup
• Microsoft Management Console (MMC) snap-in	
• Event Viewer (eventvwr.msc)	Troubleshooting Windows After Startup
• Disk Management (diskmgmt.msc)	Maintaining Windows
• Task Scheduler (taskschd.msc)	Troubleshooting Windows After Startup
• Device Manager (devmgmt.msc)	Installing Windows
• Certificate Manager (certmgr.msc)	Security Strategies

Objectives	Primary Module
• Local Users and Groups (lusrmgr.msc)	Securing and Sharing Windows Resources
• Performance Monitor (perfmon.msc)	Troubleshooting Windows After Startup
• Group Policy Editor (gpedit.msc)	Securing and Sharing Windows Resources
• Additional tools	
• System Information (msinfo32. exe)	Installing Windows
• Resource Monitor (resmon.exe)	Troubleshooting Windows After Startup
• System Configuration (msconfig. exe)	Troubleshooting Windows After Startup
• Disk Cleanup (cleanmgr.exe)	Maintaining Windows
• Disk Defragment (dfrgui.exe)	Maintaining Windows

Objectives	Primary Module
• Registry Editor (regedit.exe)	Troubleshooting Windows After Startup

1.4 Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

Objectives	Primary Module
• Internet Options	Network Security and Troubleshooting
• Devices and Printers	Securing and Sharing Windows Resources
• Programs and Features	Installing Windows
• Network and Sharing Center	Network Security and Troubleshooting
• System	Maintaining Windows
• Windows Defender Firewall	Network Security and Troubleshooting

Objectives	Primary Module
• Mail	Maintaining Windows
• Sound	Maintaining Windows
• User Accounts	Securing and Sharing Windows Resources
• Device Manager	Installing Windows
• Indexing Options	Maintaining Windows
• Administrative Tools	Troubleshooting Windows After Startup
• File Explorer Options	Maintaining Windows
• Show hidden files	Maintaining Windows
• Hide extensions	Maintaining Windows
• General options	Maintaining Windows
• View options	Maintaining Windows

Objectives	Primary Module
• Power Options	Maintaining Windows
• Hibernate	Maintaining Windows
• Power plans	Maintaining Windows
• Sleep/suspend	Maintaining Windows
• Standby	Maintaining Windows
• Choose what closing the lid does	Maintaining Windows
• Turn on fast startup	Maintaining Windows
• Universal Serial Bus (USB) selective suspend	Maintaining Windows
• Ease of Access	Installing Windows

1.5 Given a scenario, use the appropriate Windows settings.

Objectives	Primary Module
• Time and Language	Maintaining Windows
• Update and Security	Installing Windows
• Personalization	Maintaining Windows
• Apps	Installing Windows
• Privacy	Maintaining Windows
• System	Maintaining Windows
• Devices	Maintaining Windows
• Network and Internet	Maintaining Windows
• Gaming	Maintaining Windows
• Accounts	Maintaining Windows

1.6 Given a scenario, configure Microsoft Windows networking features on a client/desktop.

Objectives	Primary Module
• Workgroup vs. domain setup	
• Shared resources	Securing and Sharing Windows Resources
• Printers	Securing and Sharing Windows Resources
• File servers	Securing and Sharing Windows Resources
• Mapped drives	Securing and Sharing Windows Resources
• Local OS firewall settings	Network Security and Troubleshooting
• Application restrictions and exceptions	Network Security and Troubleshooting
• Configuration	Network Security and Troubleshooting

Objectives	Primary Module
• Client network configuration	Installing Windows
• Internet Protocol (IP) addressing scheme	Installing Windows
• Domain Name System (DNS) settings	Installing Windows
• Subnet mask	Installing Windows
• Gateway	Installing Windows
• Static vs. dynamic	Installing Windows
• Establish network connections	
• Virtual private network (VPN)	Network Security and Troubleshooting
• Wireless	Installing Windows
• Wired	Installing Windows
• Wireless wide area network (WWAN)	Network Security and Troubleshooting

Objectives	Primary Module
• Proxy settings	Network Security and Troubleshooting
• Public network vs. private network	Installing Windows
• File Explorer navigation – network paths	Securing and Sharing Windows Resources
• Metered connections and limitations	Network Security and Troubleshooting

1.7 Given a scenario, apply application installation and configuration concepts.

Objectives	Primary Module
• System requirements for applications	Installing Windows
• 32-bit vs. 64-bit dependent application requirements	Installing Windows
• Dedicated graphics card vs. integrated	Installing Windows

Objectives	Primary Module
• Video Random-access memory (VRAM) requirements	Installing Windows
• RAM requirements	Installing Windows
• Central processing unit (CPU) requirements	Installing Windows
• External hardware tokens	Installing Windows
• Storage requirements	Installing Windows
• OS requirements for applications	Installing Windows
• Application to OS compatibility	Installing Windows
• 32-bit vs. 64-bit OS	Installing Windows
• Distribution methods	Installing Windows
• Physical media vs. downloadable	Installing Windows
• ISO mountable	Installing Windows
• Other considerations for new applications	Installing Windows

Objectives	Primary Module
• Impact to device	Installing Windows
• Impact to network	Installing Windows
• Impact to operation	Installing Windows
• Impact to business	Installing Windows

1.8 Explain Common OS Types and Their Purposes.

Objectives	Primary Module
• Workstation OSs	The Complex World of IT Professionals
• Windows	The Complex World of IT Professionals
• Linux	The Complex World of IT Professionals

Objectives	Primary Module
• macOS	The Complex World of IT Professionals
• Chrome OS	The Complex World of IT Professionals
• Cell phone/tablet OSs	Mobile Device Security
• iPadOS	Mobile Device Security
• iOS	Mobile Device Security
• Android	Mobile Device Security
• Various filesystem types	
• New Technology File System (NTFS)	The Complex World of IT Professionals
• File Allocation Table 32 (FAT32)	The Complex World of IT Professionals
• Third extended filesystem (ext3)	The Complex World of IT Professionals

Objectives	Primary Module
• Fourth extended filesystem (ext4)	Linux and Scripting
• Apple File System (APFS)	Supporting macOS
• Extensible File Allocation Table (exFAT)	Maintaining Windows
• Vendor life-cycle limitations	The Complex World of IT Professionals
• End-of-life (EOL)	The Complex World of IT Professionals
• Update limitations	The Complex World of IT Professionals
• Compatibility concerns between OSs	The Complex World of IT Professionals

1.9 Given a scenario, perform OS installations and upgrades in a diverse OS environment.

Objectives	Primary Module
• Boot methods	The Complex World of IT Professionals
• USB	The Complex World of IT Professionals
• Optical media	The Complex World of IT Professionals
• Network	The Complex World of IT Professionals
• Solid-state/flash drives	The Complex World of IT Professionals
• Internet-based	The Complex World of IT Professionals
• External/hot-swappable drive	The Complex World of IT Professionals
• Internal hard drive (partition)	The Complex World of IT Professionals

Objectives	Primary Module
• Types of installations	The Complex World of IT Professionals
• Upgrade	Installing Windows
• Recovery partition	Troubleshooting Windows Startup
• Clean install	Installing Windows
• Image deployment	Installing Windows
• Repair installation	Troubleshooting Windows Startup
• Remote network installation	Installing Windows
• Other considerations	Installing Windows
• Third-party drivers	The Complex World of IT Professionals
• Partitioning	The Complex World of IT Professionals

Objectives	Primary Module
• GUID [globally unique identifier] Partition Table (GPT)	The Complex World of IT Professionals
• Master boot record (MBR)	The Complex World of IT Professionals
• Drive format	The Complex World of IT Professionals
• Upgrade considerations	Installing Windows
• Backup files and user preferences	Installing Windows
• Application and driver support/backward compatibility	Installing Windows
• Hardware compatibility	Installing Windows
• Feature updates	The Complex World of IT Professionals
• Product life cycle	The Complex World of IT Professionals

1.10 Identify common features and tools of the macOS/desktop OS.

Objectives	Primary Module
• Installation and uninstallation of applications	Supporting macOS
• File types	Supporting macOS
• .dmg	Supporting macOS
• .pkg	Supporting macOS
• .app	Supporting macOS
• App Store	Supporting macOS
• Uninstallation process	Supporting macOS
• Apple ID and corporate restrictions	Supporting macOS
• Best practices	Supporting macOS
• Backups	Supporting macOS
• Antivirus	Supporting macOS

Objectives	Primary Module
• Updates/patches	Supporting macOS
• System Preferences	Supporting macOS
• Displays	Supporting macOS
• Networks	Supporting macOS
• Printers	Supporting macOS
• Scanners	Supporting macOS
• Privacy	Supporting macOS
• Accessibility	Supporting macOS
• Time Machine	Supporting macOS
• Features	Supporting macOS
• Multiple desktops	Supporting macOS

Objectives	Primary Module
• Mission Control	Supporting macOS
• Keychain	Supporting macOS
• Spotlight	Supporting macOS
• iCloud	Supporting macOS
• Gestures	Supporting macOS
• Finder	Supporting macOS
• Remote Disc	Supporting macOS
• Dock	Supporting macOS
• Disk Utility	Supporting macOS
• FileVault	Supporting macOS
• Terminal	Supporting macOS

Objectives	Primary Module
• Force Quit	Supporting macOS

1.11 Identify common features and tools of the Linux client/desktop OS.

Objectives	Primary Module
• Common commands	Linux and Scripting
• ls	Linux and Scripting
• pwd	Linux and Scripting
• mv	Linux and Scripting
• cp	Linux and Scripting
• rm	Linux and Scripting
• chmod	Linux and Scripting
• chown	Linux and Scripting

Objectives	Primary Module
• su/sudo	Linux and Scripting
• apt-get	Linux and Scripting
• yum	Linux and Scripting
• ip	Linux and Scripting
• df	Linux and Scripting
• grep	Linux and Scripting
• ps	Linux and Scripting
• man	Linux and Scripting
• top	Linux and Scripting
• find	Linux and Scripting
• dig	Linux and Scripting

Objectives	Primary Module
• cat	Linux and Scripting
• nano	Linux and Scripting
• Best practices	Linux and Scripting
• Backups	Linux and Scripting
• Antivirus	Linux and Scripting
• Updates/patches	Linux and Scripting
• Tools	Linux and Scripting
• Shell/terminal	Linux and Scripting
• Samba	Linux and Scripting

2.0 Security

2.1 Summarize Various Security Measures and Their Purposes.

Objectives	Primary Module
• Physical security	Security Strategies
• Access control vestibule	Security Strategies
• Badge reader	Security Strategies
• Video surveillance	Security Strategies
• Alarm systems	Security Strategies
• Motion sensors	Security Strategies
• Door locks	Security Strategies
• Equipment locks	Security Strategies
• Guards	Security Strategies
• Bollards	Security Strategies
• Fences	Security Strategies
• Physical security for staff	Security Strategies

Objectives	Primary Module
• Key fobs	Security Strategies
• Smart cards	Security Strategies
• Keys	Security Strategies
• Biometrics	Security Strategies
• Retina scanner	Security Strategies
• Fingerprint scanner	Security Strategies
• Palmprint scanner	Security Strategies
• Lighting	Security Strategies
• Magnetometers	Security Strategies
• Logical security	Security Strategies
• Principle of least privilege	Security Strategies
• Access control lists (ACLs)	Security Strategies

Objectives	Primary Module
• Multifactor authentication (MFA)	Security Strategies
• Email	Security Strategies
• Hard token	Security Strategies
• Soft token	Security Strategies
• Short message service (SMS)	Security Strategies
• Voice call	Security Strategies
• Authenticator application	Security Strategies
• Mobile device management (MDM)	Mobile Device Security
• Active Directory	Securing and Sharing Windows Resources
• Login script	Securing and Sharing Windows Resources

Objectives	Primary Module
• Domain	Securing and Sharing Windows Resources
• Group Policy/updates	Securing and Sharing Windows Resources
• Organizational units	Securing and Sharing Windows Resources
• Home folder	Securing and Sharing Windows Resources
• Folder redirection	Securing and Sharing Windows Resources
• Security groups	Securing and Sharing Windows Resources

2.2 Compare and contrast wireless security protocols and authentication methods.

Objectives	Primary Module
• Protocols and encryption	Network Security and Troubleshooting
• WiFi Protected Access 2 (WPA2)	Network Security and Troubleshooting
• WPA3	Network Security and Troubleshooting
• Temporal Key Integrity Protocol (TKIP)	Network Security and Troubleshooting
• Advanced Encryption Standard (AES)	Network Security and Troubleshooting
• Authentication	Network Security and Troubleshooting
• Remote Authentication Dial-In User Service (RADIUS)	Network Security and Troubleshooting
• Terminal Access Controller Access-Control System (TACACS+)	Network Security and Troubleshooting

Objectives	Primary Module
• Kerberos	Network Security and Troubleshooting
• Multifactor	Security Strategies

2.3 Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.

Objectives	Primary Module
• Malware	Security Strategies
• Trojan	Security Strategies
• Rootkit	Security Strategies
• Virus	Security Strategies
• Spyware	Security Strategies
• Ransomware	Security Strategies
• Keylogger	Security Strategies

Objectives	Primary Module
• Boot sector virus	Security Strategies
• Cryptominers	Security Strategies
• Tools and methods	Security Strategies
• Recovery console	Security Strategies
• Antivirus	Security Strategies
• Anti-malware	Security Strategies
• Software firewalls	Security Strategies
• Anti-phishing training	Security Strategies
• User education regarding common threats	Security Strategies
• OS reinstallation	Security Strategies

2.4 Explain common social-engineering attacks, threats, and vulnerabilities.

Objectives	Primary Module
• Social engineering	Security Strategies
• Phishing	Security Strategies
• Vishing	Security Strategies
• Shoulder surfing	Security Strategies
• Whaling	Security Strategies
• Tailgating	Security Strategies
• Impersonation	Security Strategies
• Dumpster diving	Security Strategies
• Evil twin	Security Strategies
• Threats	Security Strategies
• Distributed denial of service (DDoS)	Security Strategies
• Denial of service (DoS)	Security Strategies

Objectives	Primary Module
• Zero-day attack	Security Strategies
• Spoofing	Security Strategies
• On-path attack	Security Strategies
• Brute-force attack	Security Strategies
• Dictionary attack	Security Strategies
• Insider threat	Security Strategies
• Structured Query Language (SQL) injection	Security Strategies
• Cross-site scripting (XSS)	Security Strategies
• Vulnerabilities	Security Strategies
• Non-compliant systems	Security Strategies
• Unpatched systems	Security Strategies

Objectives	Primary Module
• Unprotected systems (missing antivirus/missing firewall)	Security Strategies
• EOL OSs	Security Strategies
• Bring your own device (BYOD)	Security Strategies

2.5 Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

Objectives	Primary Module
• Defender Antivirus	Security Strategies
• Activate/deactivate	Security Strategies
• Updated definitions	Security Strategies
• Firewall	Network Security and Troubleshooting
• Activate/deactivate	Network Security and

Objectives	Primary Module
	Troubleshooting
• Port security	Network Security and Troubleshooting
• Application security	Network Security and Troubleshooting
• Users and groups	Securing and Sharing Windows Resources
• Local vs. Microsoft account	Installing Windows
• Standard account	Installing Windows
• Administrator	Installing Windows
• Guest user	Securing and Sharing Windows Resources
• Power user	Securing and Sharing Windows Resources
• Login OS options	Securing and Sharing Windows Resources

Objectives	Primary Module
• Username and password	Securing and Sharing Windows Resources
• Personal identification number (PIN)	Securing and Sharing Windows Resources
• Fingerprint	Securing and Sharing Windows Resources
• Facial recognition	Securing and Sharing Windows Resources
• Single sign-on (SSO)	Installing Windows
• NTFS vs. share permissions	Securing and Sharing Windows Resources
• File and folder attributes	Securing and Sharing Windows Resources
• Inheritance	Securing and Sharing Windows Resources

Objectives	Primary Module
• Run as administrator vs. standard user	Installing Windows
• User Account Control (UAC)	Installing Windows
• BitLocker	Securing and Sharing Windows Resources
• BitLocker To Go	Securing and Sharing Windows Resources
• Encrypting File System (EFS)	Securing and Sharing Windows Resources

2.6 Given a scenario, configure a workstation to meet best practices for security.

Objectives	Primary Module
• Data-at-rest encryption	Securing and Sharing Windows Resources
• Password best practices	Securing and Sharing Windows Resources

Objectives	Primary Module
• Complexity requirements	Securing and Sharing Windows Resources
• Length	Securing and Sharing Windows Resources
• Character types	Securing and Sharing Windows Resources
• Expiration requirements	Securing and Sharing Windows Resources
• Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords	Securing and Sharing Windows Resources
• End-user best practices	Security Strategies
• Use screensaver locks	Security Strategies
• Log off when not in use	Security Strategies
• Secure/protect critical hardware (e.g., laptops)	Security Strategies
• Secure personally identifiable information (PII) and passwords	Security Strategies

Objectives	Primary Module
• Account management	Securing and Sharing Windows Resources
• Restrict user permissions	Securing and Sharing Windows Resources
• Restrict login times	Securing and Sharing Windows Resources
• Disable guest account	Securing and Sharing Windows Resources
• Use failed attempts lockout	Securing and Sharing Windows Resources
• Use timeout/screen lock	Securing and Sharing Windows Resources
• Change default administrator’s user account/password	Securing and Sharing Windows Resources
• Disable AutoRun	Securing and Sharing Windows Resources

Objectives	Primary Module
• Disable AutoPlay	Securing and Sharing Windows Resources

2.7 Explain common methods for securing mobile and embedded devices.

Objectives	Primary Module
• Screen locks	Mobile Device Security
• Facial recognition	Mobile Device Security
• PIN codes	Mobile Device Security
• Fingerprint	Mobile Device Security
• Pattern	Mobile Device Security
• Swipe	Mobile Device Security
• Remote wipes	Mobile Device Security
• Locator applications	Mobile Device Security

Objectives	Primary Module
• OS updates	Mobile Device Security
• Device encryption	Mobile Device Security
• Remote backup applications	Mobile Device Security
• Failed login attempts restrictions	Mobile Device Security
• Antivirus/anti-malware	Mobile Device Security
• Firewalls	Mobile Device Security
• Policies and procedures	Mobile Device Security
• BYOD vs. corporate owned	Mobile Device Security
• Profile security requirements	Mobile Device Security
• Internet of Things (IoT)	Network Security and Troubleshooting

2.8 Given a scenario, use common data destruction and disposal methods.

Objectives	Primary Module
• Physical destruction	Security Strategies
• Drilling	Security Strategies
• Shredding	Security Strategies
• Degaussing	Security Strategies
• Incinerating	Security Strategies
• Recycling or repurposing best practices	Security Strategies
• Erasing/wiping	Security Strategies
• Low-level formatting	Security Strategies
• Standard formatting	Security Strategies
• Outsourcing concepts	Security Strategies
• Third-party vendor	Security Strategies

Objectives	Primary Module
• Certification of destruction/recycling	Security Strategies

2.9 Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

Objectives	Primary Module
• Home router settings	Network Security and Troubleshooting
• Change default passwords	Network Security and Troubleshooting
• IP filtering	Network Security and Troubleshooting
• Firmware updates	Network Security and Troubleshooting
• Content filtering	Network Security and Troubleshooting

Objectives	Primary Module
• Physical placement/secure locations	Network Security and Troubleshooting
• Dynamic Host Configuration Protocol (DHCP) reservations	Network Security and Troubleshooting
• Static wide-area network (WAN) IP	Network Security and Troubleshooting
• Universal Plug and Play (UPnP)	Network Security and Troubleshooting
• Screened subnet	Network Security and Troubleshooting
• Wireless specific	Network Security and Troubleshooting
• Changing the service set identifier (SSID)	Network Security and Troubleshooting
• Disabling SSID broadcast	Network Security and Troubleshooting

Objectives	Primary Module
• Encryption settings	Network Security and Troubleshooting
• Disabling guest access	Network Security and Troubleshooting
• Changing channels	Network Security and Troubleshooting
• Firewall settings	Network Security and Troubleshooting
• Disabling unused ports	Network Security and Troubleshooting
• Port forwarding/mapping	Network Security and Troubleshooting

2.10 Given a scenario, install and configure browsers and relevant security settings.

Objectives	Primary Module
• Browser download/installation	Network Security and Troubleshooting
• Trusted sources	Network Security and Troubleshooting
• Hashing	Network Security and Troubleshooting
• Untrusted sources	Network Security and Troubleshooting
• Extensions and plug-ins	Network Security and Troubleshooting
• Trusted sources	Network Security and Troubleshooting
• Untrusted sources	Network Security and Troubleshooting
• Password managers	Network Security and Troubleshooting

Objectives	Primary Module
• Secure connections/sites – valid certificates	Network Security and Troubleshooting
• Settings	Network Security and Troubleshooting
• Pop-up blocker	Network Security and Troubleshooting
• Clearing browsing data	Network Security and Troubleshooting
• Clearing cache	Network Security and Troubleshooting
• Private-browsing mode	Network Security and Troubleshooting
• Sign-in/browser data synchronization	Network Security and Troubleshooting
• Ad blockers	Network Security and Troubleshooting

3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS problems.

Objectives	Primary Module
• Common symptoms	
• Blue screen of death (BSOD)	Troubleshooting Windows Startup
• Sluggish performance	Troubleshooting Windows After Startup
• Boot problems	Troubleshooting Windows Startup
• Frequent shutdowns	Troubleshooting Windows Startup
• Services not starting	Troubleshooting Windows After Startup
• Applications crashing	Troubleshooting Windows After Startup

Objectives	Primary Module
• Low memory warnings	Troubleshooting Windows After Startup
• USB controller resource warnings	Troubleshooting Windows After Startup
• System instability	Troubleshooting Windows After Startup
• No OS found	Troubleshooting Windows Startup
• Slow profile load	Troubleshooting Windows Startup
• Time drift	Troubleshooting Windows After Startup
• Common troubleshooting steps	
• Reboot	Troubleshooting Windows After Startup
• Restart services	Troubleshooting Windows After Startup

Objectives	Primary Module
• Uninstall/reinstall/update applications	Troubleshooting Windows After Startup
• Add resources	Troubleshooting Windows After Startup
• Verify requirements	Troubleshooting Windows After Startup
• System file check	Troubleshooting Windows After Startup
• Repair Windows	Troubleshooting Windows After Startup
• Restore	Troubleshooting Windows After Startup
• Reimage	Troubleshooting Windows Startup
• Roll back updates	Troubleshooting Windows After Startup

Objectives	Primary Module
• Rebuild Windows profiles	Troubleshooting Windows Startup

3.2 Given a scenario, troubleshoot common personal computer (PC) security issues.

Objectives	Primary Module
• Common symptoms	Security Strategies
• Unable to access the network	Security Strategies
• Desktop alerts	Security Strategies
• False alerts regarding antivirus protection	Security Strategies
• Altered system or personal files	Security Strategies
• Missing/renamed files	Security Strategies
• Unwanted notifications within the OS	Security Strategies
• OS update failures	Security Strategies

Objectives	Primary Module
• Browser-related symptoms	Security Strategies
• Random/frequent pop-ups	Security Strategies
• Certificate warnings	Security Strategies
• Redirection	Security Strategies

3.3 Given a scenario, use best practice procedures for malware removal.

Objectives	Primary Module
1. Investigate and verify malware symptoms	Security Strategies
2. Quarantine infected systems	Security Strategies
3. Disable System Restore in Windows	Security Strategies
4. Remediate infected systems	Security Strategies
a. Update anti-malware software	Security Strategies

Objectives	Primary Module
b. Scanning and removal techniques (e.g., safe mode, preinstallation environment)	Security Strategies
5. Schedule scans and run updates	Security Strategies
6. Enable System Restore and create a restore point in Windows	Security Strategies
7. Educate the end user	Security Strategies

3.4 Given a scenario, troubleshoot common mobile OS and application issues.

Objectives	Primary Module
• Common symptoms	Mobile Device Security
• Application fails to launch	Mobile Device Security
• Application fails to close/crashes	Mobile Device Security

Objectives	Primary Module
• Application fails to update	Mobile Device Security
• Slow to respond	Mobile Device Security
• OS fails to update	Mobile Device Security
• Battery life issues	Mobile Device Security
• Randomly reboots	Mobile Device Security
• Connectivity issues	Mobile Device Security
• Bluetooth	Mobile Device Security
• WiFi	Mobile Device Security
• Near-field communication (NFC)	Mobile Device Security
• AirDrop	Mobile Device Security
• Screen does not autorotate	Mobile Device Security

3.5 Given a scenario, troubleshoot common mobile OS and application security issues.

Objectives	Primary Module
• Security concerns	Mobile Device Security
• Android package (APK) source	Mobile Device Security
• Developer mode	Mobile Device Security
• Root access/jailbreak	Mobile Device Security
• Bootleg/malicious application	Mobile Device Security
• Application spoofing	Mobile Device Security
• Common symptoms	Mobile Device Security
• High network traffic	Mobile Device Security
• Sluggish response time	Mobile Device Security
• Data-usage limit notification	Mobile Device Security
• Limited Internet connectivity	Mobile Device Security

Objectives	Primary Module
• No Internet connectivity	Mobile Device Security
• High number of ads	Mobile Device Security
• Fake security warnings	Mobile Device Security
• Unexpected application behavior	Mobile Device Security
• Leaked personal files/data	Mobile Device Security

4.0 Operational Procedures

4.1 Given a scenario, implement best practices associated with documentation and support systems information management.

Objectives	Primary Module
• Ticketing systems	The Complex World of IT Professionals
• User information	The Complex World of IT

Objectives	Primary Module
	Professionals
• Device information	The Complex World of IT Professionals
• Description of problems	The Complex World of IT Professionals
• Categories	The Complex World of IT Professionals
• Severity	The Complex World of IT Professionals
• Escalation levels	The Complex World of IT Professionals
• Clear, concise written communication	The Complex World of IT Professionals
• Problem description	The Complex World of IT Professionals
• Progress notes	The Complex World of IT

Objectives	Primary Module
	Professionals
• Problem resolution	The Complex World of IT Professionals
• Asset management	The Complex World of IT Professionals
• Inventory lists	The Complex World of IT Professionals
• Database system	The Complex World of IT Professionals
• Asset tags and IDs	The Complex World of IT Professionals
• Procurement life cycle	The Complex World of IT Professionals
• Warranty and licensing	The Complex World of IT Professionals
• Assigned users	The Complex World of IT

Objectives	Primary Module
	Professionals
• Types of documents	The Complex World of IT Professionals
• Acceptable use policy (AUP)	The Complex World of IT Professionals
• Network topology diagram	The Complex World of IT Professionals
• Regulatory compliance requirements	The Complex World of IT Professionals
• Splash screens	The Complex World of IT Professionals
• Incident reports	Security Strategies
• Standard operating procedures	The Complex World of IT Professionals
• Procedures for custom installation of software package	The Complex World of IT Professionals

Objectives	Primary Module
• New-user setup checklist	The Complex World of IT Professionals
• End-user termination checklist	The Complex World of IT Professionals
• Knowledge base/articles	The Complex World of IT Professionals

4.2 Explain basic change-management best practices.

Objectives	Primary Module
• Documented business processes	The Complex World of IT Professionals
• Rollback plan	The Complex World of IT Professionals
• Sandbox testing	The Complex World of IT Professionals
• Responsible staff member	The Complex World of IT Professionals

Objectives	Primary Module
• Change management	The Complex World of IT Professionals
• Request forms	The Complex World of IT Professionals
• Purpose of the change	The Complex World of IT Professionals
• Scope of the change	The Complex World of IT Professionals
• Date and time of the change	The Complex World of IT Professionals
• Affected systems/impact	The Complex World of IT Professionals
• Risk analysis	The Complex World of IT Professionals
• Risk level	The Complex World of IT Professionals

Objectives	Primary Module
• Change board approvals	The Complex World of IT Professionals
• End-user acceptance	The Complex World of IT Professionals

4.3 Given a scenario, implement workstation backup and recovery methods.

Objectives	Primary Module
• Backup and recovery	Maintaining Windows
• Full	Maintaining Windows
• Incremental	Maintaining Windows
• Differential	Maintaining Windows
• Synthetic	Maintaining Windows
• Backup testing	Maintaining Windows

Objectives	Primary Module
• Frequency	Maintaining Windows
• Backup rotation schemes	Maintaining Windows
• On site vs. off site	Maintaining Windows
• Grandfather-father-son (GFS)	Maintaining Windows
• 3-2-1 backup rule	Maintaining Windows

4.4 Given a scenario, use common safety procedures.

Objectives	Primary Module
• Electrostatic discharge (ESD) straps	Safety Procedures and Environmental Concerns
• ESD mats	Safety Procedures and Environmental Concerns
• Equipment grounding	Safety Procedures and Environmental Concerns

Objectives	Primary Module
• Proper power handling	Safety Procedures and Environmental Concerns
• Proper component handling and storage	Safety Procedures and Environmental Concerns
• Antistatic bags	Safety Procedures and Environmental Concerns
• Compliance with government regulations	Safety Procedures and Environmental Concerns
• Personal safety	Safety Procedures and Environmental Concerns
• Disconnect power before repairing PC	Safety Procedures and Environmental Concerns
• Lifting techniques	Safety Procedures and Environmental Concerns
• Electrical fire safety	Safety Procedures and Environmental Concerns

Objectives	Primary Module
• Safety goggles	Safety Procedures and Environmental Concerns
• Air filtration mask	Safety Procedures and Environmental Concerns

4.5 Summarize environmental impacts and local environmental controls.

Objectives	Primary Module
• Material safety data sheet (MSDS)/documentation for handling and disposal	Safety Procedures and Environmental Concerns
• Proper battery disposal	Safety Procedures and Environmental Concerns
• Proper toner disposal	Safety Procedures and Environmental Concerns
• Proper disposal of other devices and assets	Safety Procedures and Environmental Concerns

Objectives	Primary Module
• Temperature, humidity-level awareness, and proper ventilation	Safety Procedures and Environmental Concerns
• Location/equipment placement	Safety Procedures and Environmental Concerns
• Dust cleanup	Safety Procedures and Environmental Concerns
• Compressed air/vacuums	Safety Procedures and Environmental Concerns
• Power surges, under-voltage events, and power failures	Safety Procedures and Environmental Concerns
• Battery backup	Safety Procedures and Environmental Concerns
• Surge suppressor	Safety Procedures and Environmental Concerns

4.6 Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

Objectives	Primary Module
• Incident response	Security Strategies
• Chain of custody	Security Strategies
• Inform management/law enforcement as necessary	Security Strategies
• Copy of drive (data integrity and preservation)	Security Strategies
• Documentation of incident	Security Strategies
• Licensing/digital rights management (DRM)/end-user license agreement (EULA)	Security Strategies
• Valid licenses	Security Strategies
• Non-expired licenses	Security Strategies
• Personal use license vs. corporate use license	Security Strategies
• Open-source license	Security Strategies
• Regulated data	Security Strategies

Objectives	Primary Module
• Credit card transactions	Security Strategies
• Personal government-issued information	Security Strategies
• PII	Security Strategies
• Healthcare data	Security Strategies
• Data retention requirements	Security Strategies

4.7 Given a scenario, use proper communication techniques and professionalism.

Objectives	Primary Module
• Professional appearance and attire	The Complex World of IT Professionals
• Match the required attire of the given environment	The Complex World of IT Professionals
• Formal	The Complex World of IT

Objectives	Primary Module
	Professionals
• Business casual	The Complex World of IT Professionals
• Use proper language and avoid jargon, acronyms, and slang, when applicable	The Complex World of IT Professionals
• Maintain a positive attitude/project confidence	The Complex World of IT Professionals
• Actively listen, take notes, and avoid interrupting the customer	The Complex World of IT Professionals
• Be culturally sensitive	The Complex World of IT Professionals
• Use appropriate professional titles, when applicable	The Complex World of IT Professionals
• Be on time (if late, contact the customer)	The Complex World of IT Professionals
• Avoid distractions	The Complex World of IT

Objectives	Primary Module
	Professionals
• Personal calls	The Complex World of IT Professionals
• Texting/social media sites	The Complex World of IT Professionals
• Personal interruptions	The Complex World of IT Professionals
• Dealing with difficult customers or situations	The Complex World of IT Professionals
• Do not argue with customers or be defensive	The Complex World of IT Professionals
• Avoid dismissing customer problems	The Complex World of IT Professionals
• Avoid being judgmental	The Complex World of IT Professionals
• Clarify customer statements (ask open-ended questions to narrow the scope of the problem,	The Complex World of IT Professionals

Objectives	Primary Module
restate the issue, or question to verify understanding)	
• Do not disclose experience via social media outlets	The Complex World of IT Professionals
• Set and meet expectations/time line and communicate status with the customer	The Complex World of IT Professionals
• Offer repair/replacement options, as needed	The Complex World of IT Professionals
• Provide proper documentation on the services provided	The Complex World of IT Professionals
• Follow up with customer/user at a later date to verify satisfaction	The Complex World of IT Professionals
• Deal appropriately with customers' confidential and private materials	The Complex World of IT Professionals
• Located on a computer, desktop, printer, etc.	The Complex World of IT Professionals

4.8 Identify the basics of scripting.

Objectives	Primary Module
• Script file types	Linux and Scripting
• .bat	Linux and Scripting
• .ps1	Linux and Scripting
• .vbs	Linux and Scripting
• .sh	Linux and Scripting
• .js	Linux and Scripting
• .py	Linux and Scripting
• Use cases for scripting	Linux and Scripting

Objectives	Primary Module
• Basic automation	Linux and Scripting
• Restarting machines	Linux and Scripting
• Remapping network drives	Linux and Scripting
• Installation of applications	Linux and Scripting
• Automated backups	Linux and Scripting
• Gathering of information/data	Linux and Scripting
• Initiating updates	Linux and Scripting
• Other considerations when using scripts	Linux and Scripting

Objectives	Primary Module
• Unintentionally introducing malware	Linux and Scripting
• Inadvertently changing system settings	Linux and Scripting
• Browser or system crashes due to mishandling of resources	Linux and Scripting

4.9 Given a scenario, use remote access technologies.

Objectives	Primary Module
• Methods/tools	Network Security and Troubleshooting
• RDP	Network Security and Troubleshooting
• VPN	Network Security and Troubleshooting

Objectives	Primary Module
• Virtual network computer (VNC)	Network Security and Troubleshooting
• Secure Shell (SSH)	Linux and Scripting
• Remote monitoring and management (RMM)	Network Security and Troubleshooting
• Microsoft Remote Assistance (MSRA)	Network Security and Troubleshooting
• Third-party tools	Network Security and Troubleshooting
• Screen-sharing software	Network Security and Troubleshooting
• Video-conferencing software	Network Security and Troubleshooting
• File transfer software	Network Security and Troubleshooting
• Desktop management software	Network Security and Troubleshooting

Objectives	Primary Module
• Security considerations of each access method	Network Security and Troubleshooting