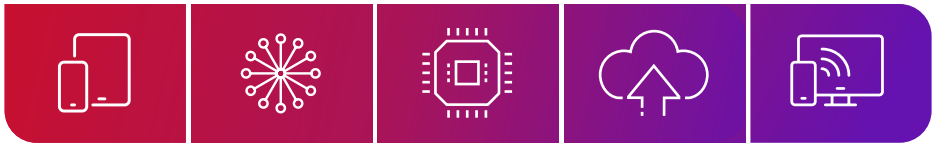
CompTIA A+ Certification Exam Objectives

EXAM NUMBER: CORE 1 (220-1201)



About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ 220-1201 certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1201) and Core 2 (220-1202). The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) certification exams will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users.
- Service components based on customer requirements.
- Understand networking basics and apply basic cybersecurity methods to mitigate threats.
- Properly and safely diagnose, resolve, and document common hardware and software issues.
- Apply troubleshooting skills and provide customer support using appropriate communication skills.
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in
- corporate environments.

EXAM ACCREDITATION

The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams are accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergo regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	A+ Core 1 (220-1201)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in an IT support specialist job role
Passing Score	675 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

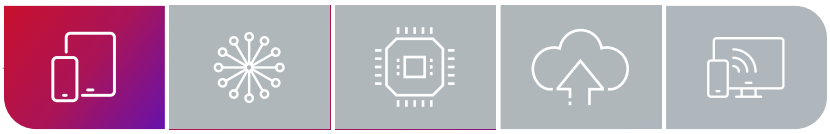
DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Mobile Devices	13%
2.0	Networking	23%
3.0	Hardware	25%
4.0	Virtualization and Cloud Computing	11%
5.0	Hardware and Network Troubleshooting	28%
Total		**100%**

TROUBLESHOOTING METHODOLOGY KNOWLEDGE

During the job task analysis workshop for the A+ 220-1200 series, subject matter experts deemed the troubleshooting methodology an effective best practice that new job incumbents should be aware of and leverage as they engage in troubleshooting new issues on the job. However, while this methodology is practical, the decision was made to not include it in the exam. While the methodology itself will not be tested, there remains an emphasis on troubleshooting within the job role context. Therefore, the troubleshooting methodology section appears here as part of this "competency standard" but does not constitute a formal objective or part of the A+ certification exam. Training institutions that prepare individuals with very little technical knowledge and experience are encouraged to leverage this methodology, especially when such individuals might be applying for their first IT job.

The troubleshooting methodology includes the following steps:

- Identify the problem.
- Establish a theory of probable cause (question the obvious).
  - Research knowledge base/internet, if applicable.
- Test the theory to determine the cause.
- Establish a plan of action to resolve the problem and implement the solution.
- Verify full system functionality and, if applicable, implement preventive measures.
- Document findings/lessons learned, actions, and outcomes.



1.0 Mobile Devices

1.1 Given a scenario, monitor mobile device hardware and use appropriate replacement techniques.

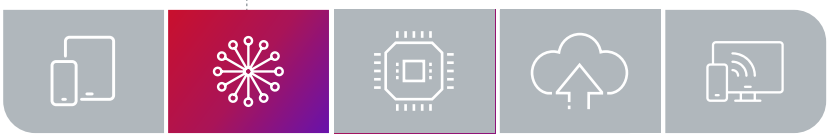
- Battery
- Keyboard/keys
- Random-access memory (RAM)
- Hard disk drive (HDD)/solid-state drive (SSD)
- Wireless cards
- Physical privacy and security components
  - Biometrics
  - Near-field scanner features
- Wi-Fi antenna connector/placement
- Camera/webcam
- Microphone

1.2 Compare and contrast accessories and connectivity options for mobile devices.

- Connection methods
  - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB
  - Lightning
  - Near-field communication (NFC)
  - Bluetooth
  - Tethering/hotspot
- Accessories
  - Stylus
  - Headsets
  - Speakers
  - Webcam
- Docking station
- Port replicator
- Trackpad/drawing pad/track points

1.3 Given a scenario, configure basic mobile device network connectivity and provide application support.

- Wireless/cellular data network (enable/disable)
  - 3G/4G/5G
  - Hotspot
  - Wi-Fi
  - Subscriber Identity Module (SIM)/eSIM
- Bluetooth
  - Enable Bluetooth
  - Enable pairing
  - Find a device for pairing
  - Enter the appropriate personal identification number (PIN) code
  - Test connectivity
- Location services
  - Global positioning system (GPS) services
  - Cellular location services
- Mobile device management (MDM)
  - Device configurations
    - Corporate
    - Bring your own device (BYOD)
  - Policy enforcement
  - Corporate applications
- Mobile device synchronization
  - Recognizing data caps
  - Calendar
  - Contacts
  - Business applications
    - Mail
    - Cloud storage



2.0 Networking

2.1 Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.

- Ports and protocols
  - 20-21 – File Transfer Protocol (FTP)
  - 22 – Secure Shell (SSH)
  - 23 – Telnet
  - 25 – Simple Mail Transfer Protocol (SMTP)
  - 53 – Domain Name System (DNS)
  - 67/68 – Dynamic Host Configuration Protocol (DHCP)
  - 80 – Hypertext Transfer Protocol (HTTP)
  - 110 – Post Office Protocol 3 (POP3)
  - 143 – Internet Mail Access Protocol (IMAP)
  - 137-139 Network Basic Input/ Output System (NetBIOS)/ NetBIOS over TCP/IP (NetBT)
  - 389 – Lightweight Directory Access Protocol (LDAP)
  - 443 – Hypertext Transfer Protocol Secure (HTTPS)
  - 445 – Server Message Block (SMB)/ Common Internet File System (CIFS)
  - 3389 – Remote Desktop Protocol (RDP)
- TCP vs. UDP

2.2 Explain wireless networking technologies.

- Frequencies
  - 2.4GHz
  - 5GHz
  - 6GHz
- Channels
  - Regulations
  - Channel selection
    - Widths
    - Frequencies
    - Bands
- Bluetooth
- 802.11 standards
- NFC
- Radio-frequency identification (RFID)

2.3 Summarize services provided by networked hosts.

- Server roles
  - DNS
  - DHCP
  - Fileshare
  - Print servers
  - Mail servers
  - Syslog
  - Web servers
  - Authentication, Authorization, and Accounting (AAA)
  - Database servers
  - Network Time Protocol (NTP)
- Internet appliances
  - Spam gateways
  - Unified threat management (UTM)
  - Load balancers
  - Proxy servers
- Legacy/embedded systems
  - Supervisory control and data acquisition (SCADA)
- Internet of Things (IoT) devices

2.4 Explain common network configuration concepts.

- DNS
  - A
  - AAAA
  - Canonical Name (CNAME)
  - Mail exchanger (MX)
  - Text (TXT)
    - Spam management
      - DomainKeys Identified Mail (DKIM)
      - Sender Policy Framework (SPF)
      - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
- DHCP
  - Leases
  - Reservations
  - Scope
  - Exclusions
- Virtual LAN [local area network] (VLAN)
- Virtual private network (VPN)

2.5 Compare and contrast common networking hardware devices.

- Routers
- Switches
  - Managed
  - Unmanaged
- Access points
- Patch panel
- Firewall
- Power over Ethernet (PoE)
  - Injectors
  - Switch
  - PoE standards
- Cable modem
- Digital subscriber line (DSL)
- Optical network terminal (ONT)
- Network interface card (NIC)
  - Physical media access control (MAC) address

2.6 Given a scenario, configure basic wired/wireless small office/home office (SOHO) networks.

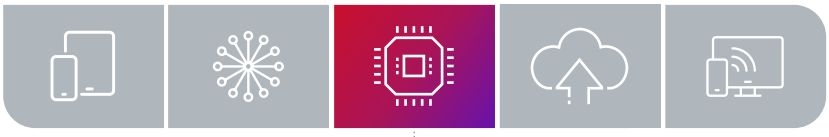
- Internet Protocol (IP) addressing
  - IPv4
    - Private addresses
    - Public addresses
  - IPv6
  - Automatic Private IP Addressing (APIPA)
  - Static
  - Dynamic
  - Subnet mask
  - Gateway

2.7 Compare and contrast internet connection types, network types, and their characteristics.

- Internet connection types
  - Satellite
  - Fiber
  - Cable
  - DSL
  - Cellular
  - Wireless internet service provider (WISP)
- Network types
  - LAN
  - Wide area network (WAN)
  - Personal area network (PAN)
  - Metropolitan area network (MAN)
  - Storage area network (SAN)
  - Wireless local area network (WLAN)

2.8 Explain networking tools and their purposes.

- Crimper
- Cable stripper
- Wi-Fi analyzer
- Toner probe
- Punchdown tool
- Cable tester
- Loopback plug
- Network tap



3.0 Hardware

3.1 Compare and contrast display components and attributes.

- Types
  - Liquid crystal display (LCD)
    - In-plane switching (IPS)
    - Twisted nematic (TN)
    - Vertical alignment (VA)
  - Organic light-emitting diode (OLED)
  - Mini light-emitting diode (Mini-LED)
- Touch screen/digitizer
- Inverter
- Attributes
  - Pixel density
  - Refresh rates
  - Screen resolution
  - Color gamut

3.2 Summarize basic cable types and their connectors, features, and purposes.

- Network cables
  - Copper
    - Categories
      - T568A/T568B standards
    - Coaxial
    - Shielded twisted pair
      - Direct burial
    - Unshielded twisted pair
  - Plenum-rated
  - Optical
    - Single-mode
    - Multimode
- Peripheral cables
  - USB 2.0
  - USB 3.0
  - Serial
  - Thunderbolt
- Video cables
  - High-definition Multimedia Interface (HDMI)
  - DisplayPort
  - Digital Visual Interface (DVI)
  - Video Graphics Array (VGA)
  - USB-C
- Hard drive cables
  - Serial Advanced Technology Attachment (SATA)
  - External SATA (eSATA)
- Adapters
- Connector types
  - RJ11
  - RJ45
  - F-type
  - Straight tip (ST)
  - Subscriber connector (SC)
  - Lucent connector (LC)
  - Punchdown block
  - MicroUSB
  - MiniUSB
  - USB-C
  - Molex
  - Lightning
  - DB9

3.3 Compare and contrast RAM characteristics.

- Form factors
  - Small Outline Dual In-line Memory Module (SODIMM)
  - Dual In-line Memory Module (DIMM)
- Double Data Rate (DDR) iterations
- Error-correcting code (ECC) vs. non-ECC RAM
- Channel configurations

3.4 Compare and contrast storage devices.

- **Hard drives**
  - Spindle speeds
  - Form factors
    - 2.5-inch
    - 3.5-inch
- **Solid-state drives**
  - Communications interfaces
    - Non-volatile Memory Express (NVMe)
    - SATA
    - Peripheral Component Interconnect Express (PCIe)
    - Serial Attached SCSI [Small Computer System Interface] (SAS)
  - Form factors
    - M.2
    - Mini-serial Advanced Technology Attachment (mSATA)
- **Drive configurations**
  - Redundant Array of Independent Disks (RAID) 0, 1, 5, 6, 10
- **Removable storage**
  - Flash drives
  - Memory cards
- **Optical drives**

3.5 Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

- **Motherboard form factors**
  - Advanced Technology Extended (ATX)
  - microATX
  - Information Technology eXtended (ITX)
- **Motherboard connector types**
  - Peripheral Component Interconnect (PCI)
  - PCIe
  - Power connectors
  - SATA
  - eSATA
  - Headers
  - M.2
- **Motherboard compatibility**
  - CPU socket types
    - Advanced Micro Devices, Inc. (AMD)
    - Intel
  - Multisocket
- **BIOS/Unified Extensible Firmware Interface (UEFI) settings**
  - Boot options
  - USB permissions
  - Trusted Platform Module (TPM) security features
  - Fan considerations
  - Secure Boot
  - Boot password
  - BIOS password
  - Temperature monitoring
- **Virtualization support**
- **Encryption**
  - TPM
  - Hardware security module (HSM)
- **CPU architecture**
  - x86/x64
  - Advanced RISC [Reduced Instruction Set Computer] Machine (ARM)
  - Core configurations
- **Expansion cards**
  - Sound card
  - Video card
  - Capture card
  - Network interface card
- **Cooling**
  - Fans
  - Heat sink
  - Thermal paste/pads
  - Liquid

3.6 Given a scenario, install the appropriate power supply.

- **Input 110–120 VAC vs. 220–240 VAC**
- **Output 3.3V vs. 5V vs. 12V**
- **20+4 pin motherboard connector**
- **Redundant power supply**
- **Modular power supply**
- **Wattage rating**
- **Energy efficiency**

3.7 Given a scenario, deploy and configure multifunction devices/printers and settings.

- Properly unbox device and consider set-up location
- Use appropriate drivers for a given operating system
  - Printer Control Language (PCL) vs. postscript
- Firmware
- Device connectivity
  - USB
  - Ethernet
  - Wireless
- Public/shared devices
  - Printer share
  - Print server
- Configuration settings
  - Duplex
  - Orientation
  - Tray settings
  - Quality
- Security
  - User authentication
  - Badging
  - Audit logs
  - Secured prints
- Network scan services
  - Email
  - SMB
  - Cloud services
- Automatic document feeder (ADF)/flatbed scanner

3.8 Given a scenario, perform appropriate printer maintenance.

- Laser
  - Maintenance: Replace toner, apply maintenance kit, calibrate, and clean
- Inkjet
  - Ink cartridge, printhead, roller, and feeder
  - Maintenance: Clean printheads, replace cartridges, calibrate, and clear jams
- Thermal
  - Feed assembly
  - Special thermal paper
  - Maintenance: Replace paper, clean heating element, and remove debris
- Impact
  - Multipart paper
  - Maintenance: Replace ribbon, printhead, and paper

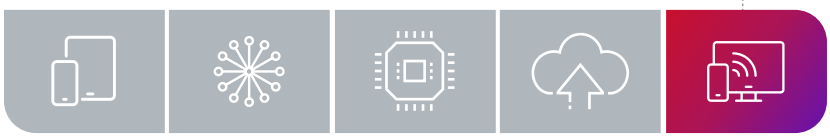
4.0 Virtualization and Cloud Computing

4.1 Explain virtualization concepts.

- Purpose of virtual machines
  - Sandbox
  - Test development
  - Application virtualization
    - Legacy software/OS
    - Cross-platform virtualization
- Requirements
  - Security
  - Network
  - Storage
- Desktop virtualization
  - Virtual Desktop Infrastructure (VDI)
- Containers
- Hypervisors
  - Type 1
  - Type 2

4.2 Summarize cloud computing concepts.

- Common cloud models
  - Private cloud
  - Public cloud
  - Hybrid cloud
  - Community cloud
  - Infrastructure as a service (IaaS)
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
- Cloud characteristics
  - Shared resources vs. dedicated resources
  - Metered utilization
    - Ingress/egress
  - Elasticity
  - Availability
  - File synchronization
  - Multitenancy



5.0 Hardware and Network Troubleshooting

5.1 Given a scenario, troubleshoot motherboards, RAM, CPUs, and power.

- **Common symptoms**
  - Power-on self-test (POST) beeps
  - Proprietary crash screens
  - Blank screen
  - No power
  - Sluggish performance
  - Overheating
  - Burning smell
  - Random shutdown
  - Application crashes
  - Unusual noise
  - Capacitor swelling
  - Inaccurate system date/time

5.2 Given a scenario, troubleshoot drive and RAID issues.

- **Common symptoms**
  - Light-emitting diode (LED) status indicators
  - Grinding noises
  - Clicking sounds
  - Bootable device not found
  - Data loss/corruption
  - RAID failure
  - Self-monitoring and Reporting Technology (S.M.A.R.T.) failure
  - Extended read/write times
  - Low performance input/output operations per second (IOPS)
  - Missing drives in OS
  - Array missing
  - Audible alarms

5.3 Given a scenario, troubleshoot video, projector, and display issues.

- **Common symptoms**
  - Incorrect input source
  - Physical cabling issues
  - Burnt-out bulb
  - Fuzzy image
  - Display burn-in
  - Dead pixels
  - Flashing screen
  - Incorrect color display
  - Audio issues
  - Dim image
  - Intermittent projector shutdown
  - Sizing issues
  - Distorted image

5.4 Given a scenario, troubleshoot common mobile device issues.

- **Common symptoms**
  - Poor battery health
  - Swollen battery
  - Broken screen
  - Improper charging
  - Poor/no connectivity
  - Liquid damage
  - Overheating
  - Digitizer issues
  - Physically damaged ports
  - Malware
  - Cursor drift/touch calibration
  - Unable to install new applications
  - Stylus does not work
  - Degraded performance

5.5 Given a scenario, troubleshoot network issues.

- **Common symptoms**
  - Intermittent wireless connectivity
  - Slow network speeds
  - Limited connectivity
  - Jitter
  - Poor Voice over Internet Protocol (VoIP) quality
  - Port flapping
  - High latency
  - External interference
  - Authentication failures
  - Intermittent internet connectivity

5.6 Given a scenario, troubleshoot printer issues.

- Lines down the printed pages
- Garbled print
- Paper jams
- Faded prints
- Paper not feeding
- Multipage misfeed
- Multiple prints pending in queue
- Speckling on printed pages
- Double/echo images on the print
- Grinding noise
- Finishing issues
  - Staple jams
  - Hole punch
- Incorrect page orientation
- Tray not recognized
- Connectivity issues
- Frozen print queue

CompTIA A+ Certification Exam Objectives

EXAM NUMBER: CORE 2 (220-1202)

About the Exam

Candidates are encouraged to use this document to help prepare for the CompTIA A+ 220-1202 certification exam. In order to receive the CompTIA A+ certification, you must pass two exams: Core 1 (220-1201) and Core 2 (220-1202). The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) certification exams will verify the successful candidate has the knowledge and skills required to:

- Install, configure, and maintain computer equipment, mobile devices, and software for end users.
- Service components based on customer requirements.
- Understand networking basics and apply basic cybersecurity methods to mitigate threats.
- Properly and safely diagnose, resolve, and document common hardware and software issues.
- Apply troubleshooting skills and provide customer support using appropriate communication skills.
- Understand the basics of scripting, cloud technologies, virtualization, and multi-OS deployments in corporate environments.

EXAM ACCREDITATION

The CompTIA A+ Core 1 (220-1201) and Core 2 (220-1202) exams are accredited by ANSI to show compliance with the ISO 17024 standard and, as such, undergo regular reviews and updates to the exam objectives.

EXAM DEVELOPMENT

CompTIA exams result from subject matter expert workshops and industry-wide survey results regarding the skills and knowledge required of an IT professional.

COMPTIA AUTHORIZED MATERIALS USE POLICY

CompTIA Certifications, LLC is not affiliated with and does not authorize, endorse, or condone utilizing any content provided by unauthorized third-party training sites (aka “brain dumps”). Individuals who utilize such materials in preparation for any CompTIA examination will have their certifications revoked and be suspended from future testing in accordance with the CompTIA Candidate Agreement. In an effort to more clearly communicate CompTIA’s exam policies on use of unauthorized study materials, CompTIA directs all certification candidates to the CompTIA Certification Exam Policies. Please review all CompTIA policies before beginning the study process for any CompTIA exam. Candidates will be required to abide by the CompTIA Candidate Agreement. If a candidate has a question as to whether study materials are considered unauthorized (aka “brain dumps”), they should contact CompTIA at examsecurity@comptia.org to confirm.

PLEASE NOTE

The lists of examples provided in bulleted format are not exhaustive lists. Other examples of technologies, processes, or tasks pertaining to each objective may also be included on the exam, although not listed or covered in this objectives document. CompTIA is constantly reviewing the content of our exams and updating test questions to be sure our exams are current, and the security of the questions is protected. When necessary, we will publish updated exams based on existing exam objectives. Please know that all related exam preparation materials will still be valid.

TEST DETAILS

Required exam	A+ Core 2 (220-1202)
Number of questions	Maximum of 90
Types of questions	Multiple-choice and performance-based
Length of test	90 minutes
Recommended experience	12 months of hands-on experience in an IT support specialist job role
Passing Score	700 (on a scale of 100–900)

EXAM OBJECTIVES (DOMAINS)

The table below lists the domains measured by this examination and the extent to which they are represented.

DOMAIN		PERCENTAGE OF EXAMINATION
1.0	Operating Systems	28%
2.0	Security	28%
3.0	Software Troubleshooting	23%
4.0	Operational Procedures	21%
Total		**100%**

NOTE ON WINDOWS 11

Versions of Microsoft® Windows® that are not end of Mainstream Support (as determined by Microsoft), up to and including Windows 11, are intended content areas of the certification. As such, objectives in which a specific version of Microsoft Windows is not indicated in the main objective title can include content related to Windows 10 and Windows 11, as it relates to the job role.

1.0 Operating Systems

1.1 Explain common operating system (OS) types and their purposes.

- Workstation systems (OSs)
  - Windows
  - Linux
  - macOS
  - Chrome OS
- Mobile OSs
  - iPadOS
  - iOS
  - Android
- Various filesystem types
  - New Technology File System (NTFS)
  - Resilient File System (ReFS)
  - File Allocation Table 32 (FAT32)
  - Fourth extended filesystem (ext4)
  - Extended filesystem (XFS)
  - Apple File System (APFS)
  - Extensible File Allocation Table (exFAT)
- Vendor life-cycle limitations
  - End-of-life (EOL)
  - Update limitations
- Compatibility concerns between operating systems

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

- Boot methods
  - Universal Serial Bus (USB)
  - Network
  - Solid-state/flash drives
  - Internet-based
  - External/hot-swappable drive
  - Internal hard drive (partition)
  - Multiboot
- Types of installations
  - Clean install
  - Upgrade
  - Image deployment
  - Remote network installation
  - Zero-touch deployment
  - Recovery partition
  - Repair installation
  - Other considerations
    - Third-party drivers
- Partitioning
  - GUID [globally unique identifier] Partition Table (GPT)
  - Master boot record (MBR)
- Drive format
- Upgrade considerations
  - Backup files and user preferences
  - Application and driver support/ backward compatibility
  - Hardware compatibility
- Feature updates
  - Product life cycle

1.3 Compare and contrast basic features of Microsoft Windows editions.

- Windows 10 editions
  - Home
  - Pro
  - Pro for Workstations
  - Enterprise
- Windows 11 editions
  - Home
  - Pro
  - Enterprise
- N versions
- Feature differences
  - Domain vs. workgroup
  - Desktop styles/user interface
  - Availability of Remote Desktop Protocol (RDP)
  - Random-access memory (RAM) support limitations
  - BitLocker
  - gpedit.msc
- Upgrade paths
  - In-place upgrade
  - Clean install
- Hardware requirements
  - Trusted Platform Module (TPM)
  - Unified Extensible Firmware Interface (UEFI)

1.4 Given a scenario, use Microsoft Windows operating system features and tools.

- Task Manager
  - Services
  - Startup
  - Performance
  - Processes
  - Users
- Microsoft Management Console (MMC) snap-in
  - Event Viewer (eventvwr.msc)
  - Disk Management (diskmgmt.msc)
  - Task Scheduler (taskschd.msc)
  - Device Manager (devmgmt.msc)
  - Certificate Manager (certmgr.msc)
  - Local User and Groups (lusrmgr.msc)
  - Performance Monitor (perfmon.msc)
  - Group Policy Editor (gpedit.msc)
- Additional tools
  - System Information (msinfo32. exe)
  - Resource Monitor (resmon.exe)
  - System Configuration (msconfig. exe)
  - Disk Cleanup (cleanmgr.exe)
  - Disk Defragment (dfrgui.exe)
  - Registry Editor (regedit.exe)

1.5 Given a scenario, use the appropriate Microsoft command-line tools.

- Navigation
  - cd
  - dir
- Network
  - ipconfig
  - ping
  - netstat
  - nslookup
  - net use
  - tracert
  - pathping
- Disk management
  - chkdsk
  - format
  - diskpart
- File management
  - md
  - rmdir
  - robocopy
- Informational
  - hostname
  - net user
  - winver
  - whoami
  - [command name] /?
- OS management
  - gpupdate
  - gpresult
  - sfc

1.6 Given a scenario, configure Microsoft Windows settings.

- Internet Options
- Devices and Printers
- Program and Features
- Network and Sharing Center
- System
- Windows Defender Firewall
- Mail
- Sound
- Device Manager
- Indexing Options
- Administrative Tools
- File Explorer Options
  - View hidden files
  - Hide extensions
  - General options
  - View options
- Power Options
  - Hibernate
  - Power plans
  - Sleep/suspend
  - Standby
  - Choose what closing the lid does
  - Turn on fast startup
  - USB selective suspend
- Ease of Access
- Time and Language
- Update and Security
- Personalization
- Apps
- Privacy
- Devices
- Network and Internet
- Gaming
- Accounts

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

- Domain joined vs. workgroup
  - Shared resources
  - Printers
  - File servers
  - Mapped drives
- Local OS firewall settings
  - Application restrictions and exceptions
  - Configuration
- Client network configuration
  - Internet Protocol (IP) addressing scheme
  - Domain Name System (DNS) settings
  - Subnet mask
  - Gateway
  - Static vs. dynamic
- Establish network connections
  - Virtual private network (VPN)
  - Wireless
  - Wired
  - Wireless wide area network (WWAN)/cellular network
- Proxy settings
- Public network vs. private network
- File Explorer navigation–network paths
- Metered connections and limitations

1.8 Explain common features and tools of the macOS/desktop operating system.

- Installation and uninstallation of applications
  - File types
    - .dmg
    - .pkg
    - .app
  - App Store
  - Uninstallation process
- System folders
  - /Applications
  - /Users
  - /Library
  - /System
  - /Users/Library
- Apple ID and corporate restrictions
- Best practices
  - Backups
  - Antivirus
  - Updates/patches
  - Rapid Security Response (RSR)
- System Settings
  - Displays
  - Networks
  - Printers
  - Scanners
  - Privacy
  - Accessibility
  - Time Machine
- Features
  - Multiple desktops
  - Mission Control
  - Keychain
  - Spotlight
  - iCloud
    - iMessage
    - FaceTime
    - Drive
  - Gestures
  - Finder
  - Dock
  - Continuity
- Disk Utility
- FileVault
- Terminal
- Force Quit

1.9 Identify common features and tools of the Linux client/desktop operating system.

- File management
  - ls
  - pwd
  - mv
  - cp
  - rm
  - chmod
  - chown
  - grep
  - find
- Filesystem management
  - fsck
  - mount
- Administrative
  - su
  - sudo
- Package management
  - apt
  - dnf
- Network
  - ip
  - ping
  - curl
  - dig
  - traceroute
- Informational
  - man
  - cat
  - top
  - ps
  - du
  - df
- Text editors
  - nano
- Common configuration files
  - /etc/passwd
  - /etc/shadow
  - /etc/hosts
  - /etc/fstab
  - /etc/resolv.conf
- OS components
  - systemd
  - kernel
  - bootloader
- Root account

1.10 Given a scenario, install applications according to requirements. .

- System requirements for applications
  - 32-bit vs. 64-bit dependent application requirements
  - Dedicated vs. integrated graphics card
  - Video random-access memory (VRAM) requirements
  - RAM requirements
  - Central processing unit (CPU) requirements
  - External hardware tokens
  - Storage requirements
  - Application to OS compatibility
- Distribution methods
  - Physical media vs. mountable ISO file
  - Downloadable package
  - Image deployment
- Impact considerations for new applications
  - Device
  - Network
  - Operation
  - Business

1.11 Given a scenario, install and configure cloud-based productivity tools. .

- Email systems
- Storage
  - Sync/folder settings
- Collaboration tools
  - Spreadsheets
  - Videoconferencing
  - Presentation tools
  - Word processing tools
  - Instant messaging
- Identity synchronization
- Licensing assignment

2.0 Security

2.1 Summarize various security measures and their purposes.

- **Physical security**
  - Bollards
  - Access control vestibule
  - Badge reader
  - Video surveillance
  - Alarm systems
  - Motion sensors
  - Door locks
  - Equipment locks
  - Security guards
  - Fences
- **Physical access security**
  - Key fobs
  - Smart cards
  - Mobile digital key
  - Keys
  - Biometrics
    - Retina scanner
    - Fingerprint scanner
    - Palm print scanner
    - Facial recognition technology (FRT)
    - Voice recognition technology
  - Lighting
  - Magnetometers
- **Logical security**
  - Principle of least privilege
  - Zero Trust model
  - Access control lists (ACLs)
  - Multifactor authentication (MFA)
    - Email
    - Hardware token
    - Authenticator application
    - Short Message Service (SMS)
    - Voice call
    - Time-based one-time password (TOTP)
    - One-time password/ passcode (OTP)
  - Security Assertions Markup Language (SAML)
  - Single sign-on (SSO)
  - Just-in-time access
    - Privileged access management (PAM)
  - Mobile device management (MDM)
  - Data loss prevention (DLP)
  - Identity access management (IAM)
  - Directory services

2.2 Given a scenario, configure and apply basic Microsoft Windows OS security settings.

- **Defender Antivirus**
  - Activate/deactivate
  - Update definitions
- **Firewall**
  - Activate/deactivate
  - Port security
  - Application security
- **User and groups**
  - Local vs. Microsoft account
  - Standard account
  - Administrator
  - Guest user
  - Power user
- **Log-in OS options**
  - Username and password
  - Personal identification number (PIN)
  - Fingerprint
  - Facial recognition
  - SSO
  - Passwordless/Windows Hello
- **NTFS vs. share permissions**
  - File and folder attributes
  - Inheritance
- **Run as administrator vs. standard user**
- **User Account Control (UAC)**
- **BitLocker**
- **BitLocker-To-Go**
- **Encrypting File System (EFS)**
- **Active Directory**
  - Joining domain
  - Assigning log-in script
  - Moving objects within organizational units
  - Assigning home folders
  - Applying Group Policy
  - Selecting security groups
  - Configuring folder redirection

2.3 Compare and contrast wireless security protocols and authentication methods.

- Protocols and encryption
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA3
  - Temporal Key Integrity Protocol (TKIP)
  - Advanced Encryption Standard (AES)
- Authentication
  - Remote Authentication Dial-in User Service (RADIUS)
  - Terminal Access Controller Access-control System (TACACS+)
  - Kerberos
  - Multifactor

2.4 Summarize types of malware and tools/methods for detection, removal, and prevention.

- Malware
  - Trojan
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Boot sector virus
  - Cryptominer
  - Stalkerware
  - Fileless
- Adware
  - Potentially unwanted program (PUP)
- Tools and methods
  - Recovery Console/ environment/modes
  - Endpoint detection and response (EDR)
  - Managed detection and response (MDR)
  - Extended detection and response (XDR)
  - Antivirus
  - Anti-malware
  - Email security gateway
  - Software firewalls
  - User education regarding common threats
    - Antiphishing training
  - OS reinstallation

2.5 Compare and contrast common social engineering attacks, threats, and vulnerabilities.

- Social engineering
  - Phishing
    - Vishing
    - Smishing
    - QR code phishing
    - Spear phishing
    - Whaling
  - Shoulder surfing
  - Tailgating
  - Impersonation
  - Dumpster diving
- Threats
  - Denial of service (DoS)
  - Distributed denial of service (DDoS)
  - Evil twin
  - Zero-day attack
  - Spoofing
  - On-path attack
  - Brute-force attack
  - Dictionary attack
  - Insider threat
  - Structured Query Language (SQL) injection
  - Cross-site scripting (XSS)
  - Business email compromise (BEC)
  - Supply chain/pipeline attack
- Vulnerabilities
  - Non-compliant systems
  - Unpatched systems
  - Unprotected systems (missing antivirus/missing firewall)
  - EOL
  - Bring your own device (BYOD)

2.6 Given a scenario, implement procedures for basic small office/home office (SOHO) malware removal.

1. Investigate and verify malware symptoms.
2. Quarantine infected system.
3. Disable System Restore in Windows Home.
4. Remediate infected systems.
5. Update anti-malware software.
6. Scan and removal techniques (e.g., safe mode, preinstallation environment)
7. Reimage/reinstall.
8. Schedule scans and run updates.
9. Enable System Restore and create a restore point in Windows Home.
10. Educate the end user.

2.7 Given a scenario, apply workstation security options and hardening techniques.

- Data-at-rest encryption
- Password considerations
  - Length
  - Character types
  - Uniqueness
  - Complexity
  - Expiration
- Basic input/output system (BIOS)/ Unified Extensible Firmware Interface (UEFI) passwords
- End-user best practices
  - Use screensaver locks
  - Log off when not in use
  - Secure/protect critical hardware (e.g., laptops)
  - Secure personally identifiable information (PII) and passwords
  - Use password managers
- Account management
  - Restrict user permissions
  - Restrict log-in times
  - Disable guest account
  - Use failed attempts lockout
  - Use timeout/screen lock
  - Apply account expiration dates
- Change default administrator's user account/password
- Disable AutoRun
- Disable unused services

2.8 Given a scenario, apply common methods for securing mobile devices.

- Hardening techniques
  - Device encryption
  - Screen locks
    - Facial recognition
    - PIN codes
    - Fingerprint
    - Pattern
    - Swipe
  - Configuration profiles
- Patch management
  - OS updates
  - Application updates
- Endpoint security software
  - Antivirus
  - Anti-malware
  - Content filtering
- Locator applications
- Remote wipes
- Remote backup applications
- Failed log-in attempts restrictions
- Policies and procedures
  - MDM
  - BYOD vs. corporate-owned devices
  - Profile security requirements

2.9 Compare and contrast common data destruction and disposal methods.

- Physical destruction of hard drives
  - Drilling
  - Shredding
  - Degaussing
  - Incineration
- Recycling or repurposing best practices
  - Erasing/wiping
  - Low-level formatting
  - Standard formatting
- Outsourcing concepts
  - Third-party vendor
  - Certification of destruction/recycling
- Regulatory and environmental requirements

2.10 Given a scenario, apply security settings on SOHO wireless and wired networks.

- **Router settings**
  - Change default passwords
  - IP filtering
  - Firmware updates
  - Content filtering
  - Physical placement/secure locations
  - Universal Plug and Play (UPnP)
  - Screened subnet
  - Configure secure management access
- **Wireless specific**
  - Changing the service set identifier (SSID)
  - Disabling SSID broadcast
  - Encryption settings
  - Configuring guest access
- **Firewall settings**
  - Disabling unused ports
  - Port forwarding/mapping

2.11 Given a scenario, configure relevant security settings in a browser.

- **Browser download/installation**
  - Trusted sources
    - Hashing
  - Untrusted sources
- **Browser patching**
- **Extensions and plug-ins**
  - Trusted sources
  - Untrusted sources
- **Password managers**
- **Secure connections/ sites–valid certificates**
- **Settings**
  - Pop-up blocker
  - Clearing browsing data
  - Clearing cache
  - Private-browsing mode
  - Sign-in/browser data synchronization
  - Ad blockers
  - Proxy
  - Secure DNS
- **Browser feature management**
  - Enable/disable
    - Plug-ins
    - Extensions
    - Features

3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS issues.

- Blue screen of death (BSOD)
- Degraded performance
- Boot issues
- Frequent shutdowns
- Services not starting
- Applications crashing
- Low memory warnings
- USB controller resource warnings
- System instability
- No OS found
- Slow profile load
- Time drift

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

- Application fails to launch
- Application fails to close/crashes
- Application fails to update
- Application fails to install
- Slow to respond
- OS fails to update
- Battery life issues
- Random reboots
- Connectivity issues
  - Bluetooth
  - Wi-Fi
  - Near-field communication (NFC)
- Screen does not autorotate

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

- Security concerns
  - Application source/unofficial application stores
  - Developer mode
  - Root access/jailbreak
  - Unauthorized/malicious application
    - Application spoofing
- Common symptoms
  - High network traffic
  - Degraded response time
  - Data-usage limit notification
  - Limited internet connectivity
  - No internet connectivity
  - High number of ads
  - Fake security warnings
  - Unexpected application behavior
  - Leaked personal files/data

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

- Common symptoms
  - Unable to access the network
  - Desktop alerts
  - False alerts regarding antivirus protection
  - Altered system or personal files
    - Missing/renamed files
    - Inability to access files
  - Unwanted notifications within the OS
  - OS updates failures
- Browser-related symptoms
  - Random/frequent pop-ups
  - Certificate warnings
  - Redirection
  - Degraded browser performance

4.0 Operational Procedures

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

- **Ticketing systems**
  - User information
  - Device information
  - Description of issues
  - Categories
  - Severity
  - Escalation levels
  - Clear, concise written communication
    - Issue description
    - Progress notes
    - Issue resolution
- **Asset management**
  - Inventory lists
  - Configuration management database (CMDB)
  - Asset tags and IDs
  - Procurement life cycle
  - Warranty and licensing
  - Assigned users
- **Types of documents**
  - Incident reports
  - Standard operating procedures (SOPs)
    - Software package custom installation procedure
  - New user/onboarding setup checklist
  - User off-boarding checklist
  - Service-level agreements (SLAs)
    - Internal
    - External/third-party
  - Knowledge base/articles

4.2 Given a scenario, apply change management procedures.

- **Documented business processes**
  - Rollback plan
  - Backup plan
  - Sandbox testing
  - Responsible staff members
- **Change management**
  - Request forms
  - Purpose of the change
  - Scope of the change
  - Change type
    - Standard change
    - Normal change
    - Emergency change
  - Date and time of change
    - Change freeze
    - Maintenance windows
  - Affected systems/impact
  - Risk analysis
    - Risk level
  - Change board approvals
  - Implementation
  - Peer review
  - End-user acceptance

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

- **Backup**
  - Full
  - Incremental
  - Differential
  - Synthetic full
- **Recovery**
  - In-place/overwrite
  - Alternative location
- **Backup testing**
  - Frequency
- **Backup rotation schemes**
  - Onsite vs. offsite
  - Grandfather-father-son (GFS)
  - 3-2-1 backup rule

4.4 Given a scenario, use common safety procedures.

- Electrostatic discharge (ESD) straps
- ESD mats
- Electrical safety
  - Equipment grounding
- Proper component handling and storage
- Cable management
- Antistatic bags
- Compliance with government regulations
- Personal safety
  - Disconnect power before repairing PC
  - Lifting techniques
  - Fire safety
  - Safety goggles
  - Air filter mask

4.5 Summarize environmental impacts and local environment controls.

- Material safety data sheet (MSDS) documentation for handling and disposal
  - Proper battery disposal
  - Proper toner disposal
  - Proper disposal of other devices and assets
- Temperature, humidity-level awareness, and proper ventilation
  - Location/equipment placement
  - Dust cleanup
  - Compressed air/vacuums
- Power surges, under-voltage events, and power losses
  - Uninterruptible power supply (UPS)
  - Surge suppressor

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

- Incident response
  - Chain of custody
  - Informing management/law enforcement as necessary
  - Copy of drive (data integrity and preservation)
  - Incident documentation
  - Order of volatility
- Licensing/digital rights management (DRM)/ end-user license agreement (EULA)
  - Valid licenses
  - Perpetual license agreement
  - Personal-use license vs. corporate-use license
  - Open-source license
- Non-disclosure agreement (NDA)/mutual non-disclosure agreement (MNDA)
- Regulated data
  - Credit card payment information
  - Personal government-issued information
  - PII
  - Healthcare data
  - Data retention requirements
- Acceptable use policy (AUP)
- Regulatory and business compliance requirements
  - Splash screens

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

- Present a professional appearance and wear appropriate attire.
  - Match the required attire of the given environment.
    - Formal
    - Business casual
- Use proper language and avoid jargon, acronyms, and slang, when applicable.
- Maintain a positive attitude/ project confidence.
- Actively listen and avoid interrupting the customer.
- Be culturally sensitive.
  - Use appropriate professional titles and designations, when applicable.
- Be on time (if late, contact the customer).
- Avoid distractions.
  - Personal calls
  - Texting/social media sites
  - Personal interruptions
- Appropriately deal with difficult customers or situations.
  - Do not argue with customer and/or be defensive.
  - Avoid dismissing customer issues.
  - Avoid being judgmental.
  - Clarify customer statements (i.e., ask open-ended questions to narrow the scope of the issue, restate the issue, or question to verify understanding).
  - Use discretion and professionalism when discussing experiences/encounters.
- Set and meet expectations/ timeline and communicate status with the customer.
  - Offer repair/replacement options, as needed.
  - Provide proper documentation on the services provided.
  - Follow up with customer/user at a later date to verify satisfaction.
- Appropriately handle customers' confidential and private materials.
  - Located on a computer, desktop, printer, etc.

4.8 Explain the basics of scripting.

- Script file types
  - .bat
  - .ps1
  - .vbs
  - .sh
  - .js
  - .py
- Use cases for scripting
  - Basic automation
  - Restarting machines
  - Remapping network drives
  - Installation of applications
  - Automated backups
  - Gathering of information/data
  - Initiating updates
- Other considerations when using scripts
  - Unintentionally introducing malware
  - Inadvertently changing system settings
  - Browser or system crashes due to mishandling of resources

4.9 Given a scenario, use remote access technologies.

- Methods/tools
  - RDP
  - VPN
  - Virtual network computer (VNC)
  - Secure Shell (SSH)
  - Remote monitoring and management (RMM)
  - Simple Protocol for Independent Computing Environments (SPICE)
  - Windows Remote Management (WinRM)
  - Third-party tools
    - Screen-sharing software
    - Videoconferencing software
    - File transfer software
    - Desktop management software
- Security considerations of each access method

4.10 Explain basic concepts related to artificial intelligence (AI).

- Application integration
- Policy
  - Appropriate use
  - Plagiarism
- Limitations
  - Bias
  - Hallucinations
  - Accuracy
- Private vs. public
  - Data security
  - Data source
  - Data privacy