CompTIA A+

Certification Exam
Core 2 Pre-draft Exam Objectives
Exam Number: Core 2 (220-1202)

- Pre-draft Exam Objectives summarize the tasks and skills identified in the Job Task Analysis (JTA) workshop that provide directional information about the upcoming exam version.
- The Draft Exam Objectives will replace the Pre-draft Exam Objectives after approximately two months when the skills have been peer-evaluated and validated through a JTA survey of job role practitioners.
- Pre-draft Exam Objectives may contain typos and errata that will be corrected during the development process.
- CompTIA will not accept feedback on the Pre-draft Exam Objectives document. If errors are found, please wait until the Draft Exam Objectives are posted, and then provide feedback using the Draft Exam Objectives Feedback form.

1.0 Operating Systems

1.1 Explain common operating system types and their purposes.

- Workstation Operating Systems
  - Windows
  - Linux
  - macOS
  - Chrome OS
- Mobile operating systems
  - iPadOS
  - iOS
  - Android
- Various file system types
  - NTFS
  - Resilient File System (ReFS)
  - FAT32
  - ext4
  - XFS
  - Apple File System (APFS)
  - exFAT
- Vendor lifecycle limitations
  - End-of-life
  - Update limitations
- Compatibility concerns between operating systems

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

- Boot methods
  - USB
  - Network
  - Solid state/flash drives
  - Internet-based
  - External/hot swappable drive
  - Internal hard drive (partition)
  - Multi-boot
- Type of installations
  - Clean install
  - Upgrade
  - Image deployment
  - Remote network installation
  - Zero-touch deployment
  - Recovery partition
  - Repair installation
  - Other considerations
    - Third-party drivers
- Partitioning
  - GPT
  - MBR
- Drive format
- Upgrade considerations
  - Backup files and user preferences
  - Application & driver support/backwards compatibility
  - Hardware compatibility
- Feature updates
  - Product lifecycle

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
  - RAM support limitations
  - BitLocker
  - gpedit.msc
- Upgrade paths
  - In-place upgrade
  - Clean install
- Hardware requirements
  - TPM
  - UEFI

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

- Task Manager
  - Services
  - Startup
  - Performance
  - Processes
  - Users
- 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
- User Accounts
- 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 & Language
- Update & Security
- Personalization
- Apps
- Privacy
- System
- Devices
- Network & 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
  - IP addressing scheme
  - DNS settings
  - Subnet mask
  - Gateway
  - Static vs. dynamic
- Establish network connections
  - VPN
  - Wireless
  - Wired
  - 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
  - RSR
- System Preferences
  - 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
- File system 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 graphics card vs. integrated
  - VRAM requirements
  - RAM requirements
  - CPU requirements
  - External hardware tokens
  - Storage requirements
  - Application to OS compatibility
- Distribution methods
  - Physical media vs. mountable ISO
  - 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
  - Video conferencing
  - 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/PIV card/CAC
  - 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 models
  - Access control lists
  - Multifactor authentication
    - Email
    - Hardware token
    - Authenticator app
    - SMS
    - Voice call
    - TOTP
    - OTP (One-time password/passcode)
  - SAML
  - SSO
  - Just-in-time access
    - Privileged access management (PAM)
  - Mobile Device Management
  - 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
- Login OS options
  - User name and password
  - PIN
  - Fingerprint
  - Facial recognition
  - Single Sign-On
  - Passwordless/Windows Hello
- NTFS vs. Share permissions
  - File and folder attributes
  - Inheritance
- Run as administrator vs. standard user
- UAC
- Bitlocker
- Bitlocker-To-Go
- EFS
- Active Directory
  - Joining domain
  - Assigning login 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
  - WPA2
  - WPA3
  - TKIP
  - AES
- Authentication
  - RADIUS
  - TACACS+
  - Kerberos
  - Multi-factor

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

- Malware
  - Trojan
  - Rootkit
  - Virus
  - Spyware
  - Ransomware
  - Keylogger
  - Boot sector virus
  - Cryptominers
  - Stalkerware
  - Fileless
- Adware

  - Potentially unwanted program (PUP)
- Tools and methods
  - Recovery console
  - Endpoint Detection & Response (EDR)
  - Managed Detection & Response (MDR)
  - Extended Detection & Response (XDR)
  - Antivirus
  - Antimalware
  - Email security gateway
  - Software firewalls
  - User education regarding common threats
    - Anti-phishing training
  - OS reinstallation

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

- Social engineering
  - Phishing
    - Vishing
    - Smishing
    - QR phishing
    - Spear phishing
    - Whaling
  - Shoulder surfing
  - Tailgating
  - Impersonation
  - Dumpster diving
- Threats
  - DoS
  - DDoS
  - Evil twin
  - Zero day
  - Spoofing
  - On-path attack
  - Brute force
  - Dictionary
  - Insider threat
  - SQL injection
  - XSS
  - Business Email Compromise (BEC)
  - Supply Chain/Pipeline attack
- Vulnerabilities
  - Non-compliant systems
  - Unpatched systems
  - Unprotected systems (missing antivirus/missing firewall)
  - End-of-life (EOL)
  - BYOD

2.6 Given a scenario, implement procedures for basic SOHO malware removal

1. Investigate and verify malware symptoms
2. Quarantine infected system
3. Disable system restore (in Windows Home)
4. Remediate infected systems
    a. Update antimalware software
    b. Scan and removal techniques (safe mode, pre-installation environment)
    c. Re-image/re-install

5. Schedule scans and run updates
6. Enable system restore and create restore point (in Windows Home)
7. Educate 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
- BIOS/UEFI passwords
- End-user best practices
  - Screen saver locks
  - Log off when not in use
  - Securing/protecting critical hardware (e.g. laptops)
  - Secure PII and passwords
  - Password Manager
- Account management
  - Restricting user permissions
  - Login time restrictions
  - Disabling guest account
  - Failed attempts lockout
  - Timeout/screen lock
  - Account expiration dates
- Change default admin user account/password
- Disable Autorun
- Disabling 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
  - App updates
- Endpoint security software
  - Antivirus
  - Antimalware
  - Content filtering
- Locator applications
- Remote wipes
- Remote backup applications
- Failed login attempts restrictions
- Policies and procedures
  - MDM
  - BYOD vs. corporate owned
  - 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
  - UPnP
  - DMZ
  - Configure secure management access
- Wireless specific
  - Changing the SSID
  - Disable 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 & Plug-ins
  - Trusted sources
  - Untrusted sources
- Password managers
- Secure connections/sites – valid certificates
- Settings
  - Popup blocker
  - Clearing browsing data
  - Clearing cache
  - Private-browsing mode
  - Sign-in/browser data synchronization
  - Adblockers
  - Proxy
  - Secure DNS

- Browser feature management
  - Enable/disable
    - Plugins
    - Extensions
    - Features

3.0 Software Troubleshooting

3.1 Given a scenario, troubleshoot common Windows OS problems.

- BSOD
- Degraded performance
- Boot problems
- Frequent shut downs
- 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
- Randomly reboots
- Connectivity issues
  - Bluetooth
  - Wi-Fi
  - NFC
- Screen does not auto-rotate

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

- Security concerns
  - Application source/Unofficial app stores
  - Developer mode
  - Root access/Jailbreak
  - Unauthorized/malicious application
    - App 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 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 popups
  - 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 problems
  - Categories
  - Severity
  - Escalation levels
  - Clear, concise written communication
    - Problem description
    - Progress notes
    - Problem resolution
- Asset management
  - Inventory lists
  - Configuration management database (CMDB)
  - Asset tags and IDs
  - Procurement lifecycle
  - 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
- Knowledgebase/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
  - GFS
  - 3-2-1 backup rule

4.4 Given a scenario, use common safety procedures.

- 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.

- MSDS documentation for handling and disposal
  - Proper battery disposal
  - Proper toner disposal
  - Disposal of other devices and assets
- Temperature, humidity level awareness and proper ventilation
  - Location/equipment placement
  - Cleaning up dust
  - Compressed air/vacuums
- Power surges, brownouts, blackouts
  - 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
  - Inform management/law enforcement as necessary
  - Copy of drive (data integrity and preservation)
  - Documentation of incident
  - Order of volatility
- Licensing / DRM / EULA
  - Valid licenses
  - Perpetual license agreement
  - Personal use license vs. corporate use
  - Open source license
- Non-disclosure agreement (NDA)/mutual non-disclosure agreement (MNDA)
- Regulated Data
  - Credit card payment information
  - Personal government-issued information
  - Personally Identifiable Information
  - Healthcare data
  - Data retention requirements
- Acceptable Use Policy
- Regulatory and business compliance requirements
  - Splash screens

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

- Professional appearance and 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
- Dealing with difficult customers or situations
  - Do not argue with customer and/or be defensive
  - Avoid dismissing customer problems

    - Avoid being judgmental
    - Clarify customer statements (ask open-ended questions to narrow the scope of the problem, 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
- Appropriate handling of 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
    - VNC
    - SSH
    - RMM
    - SPICE
    - WinRM
    - Third-party tools
        - Screensharing software
        - Video conferencing 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