Computer Systems 2

Exam Information

Exam number
885

Items
45

Points
45

Prerequisites
Computer Systems

Recommended course length
One semester

National Career Cluster
Information Technology

Performance standards
Included (Optional)

Certificate available
Yes

Description

The Computer Systems 2 industry certification exam assesses necessary competencies for an entry-level IT professional, including troubleshooting, optimizing, diagnosing, and performing preventive maintenance of basic personal computer hardware and operating systems.

Exam Blueprint

Standard	Percentage of exam
1. Operating Systems	47%
2. Security	13%
3. Software Troubleshooting	27%
4. Operational Procedures	13%

STANDARD 1

Operating Systems

Objective 1 Understand common operating systems and their purposes.

1. Software compatibility
2. Workstation operating systems
    a. Microsoft Windows
    b. Apple Macintosh OS
    c. Linux Distributions
3. Cell Phone/tablet operating systems
    a. Microsoft Windows
    b. Android
    c. iOS
    d. Chrome OS
4. Vendor specific limitations

Objective 2 Understand general OS installation considerations and upgrade methods.

1. Boot Methods
    a. Optical disc (CD-ROM, DVD, Blu-ray)
    b. External drive/flash drive (USB/eSATA)
    c. Network boot (PXE)
    d. Internal fixed disk (HDD/SSD)
    e. Internal hard drive (partition)
2. Type of installations
    a. Unattended installation
    b. In-place upgrade
    c. Clean install
    d. Repair installation
    e. Multiboot
    f. Remote network installation
    g. Image deployment
    h. Recovery partition
    i. Refresh/restore
3. Partitioning
    a. Dynamic
    b. Basic

    c. Primary
    d. Extended
    e. Logical
    f. GPT
4. File system types/formatting
    a. ExFAT
    b. FAT32
    c. NTFS
    d. CDFS
    e. NFS
    f. XFS
    g. ext3, ext4, ext4 journaling
    h. HFS
    i. Swap partition
    j. Quick format vs. full format
5. Load alternate third-party drivers when necessary
6. Workgroup vs. Domain setup
7. Time/date/region/language settings
8. Driver installation, software, and Windows updates
9. Factory recovery partition
10. Properly formatted boot drive with the correct partitions/format
11. Prerequisites/hardware compatibility
12. Application compatibility
13. OS compatibility/upgrade path

Objective 3 Demonstrate the use of Microsoft command line tools.

1. Navigation
    a. dir
    b. cd
    c. ..
2. ipconfig
3. ping
4. tracert
5. netstat
6. nslookup
7. shutdown
8. dism

9. sfc
10. chkdsk
11. diskpart
12. taskkill
13. gpupdate
14. gpresult
15. format
16. copy
17. xcopy
18. robocopy
19. net use
20. net user
21. [command name] /?
22. Commands available with standard privileges vs. administrative privileges

Objective 4 Demonstrate the use of Microsoft operating system features and tools.

1. Administrative
    a. Computer Management
    b. Device Manager
    c. Local Users and Groups
    d. Local Security Policy
    e. Performance Monitor
    f. Services
    g. System Configuration
    h. Task Scheduler
    i. Component Services
    j. Data Sources
    k. Print Management
    l. Windows Memory Diagnostics
    m. Windows Firewall
    n. Advanced Security
    o. Event Viewer
    p. User Account Management
2. MSConfig
    a. General
    b. Boot
    c. Services

    d. Startup
    e. Tools
3. Task Manager
    a. Applications
    b. Processes
    c. Performance
    d. Networking
    e. Users
4. Disk Management
    a. Drive status
    b. Mounting
    c. Initializing
    d. Extending partitions
    e. Splitting partitions
    f. Shrink partitions
    g. Assigning/changing drive letters
    h. Adding drives
    i. Adding arrays
    j. Storage spaces
5. System Utilities
    a. Regedit
    b. Command
    c. Services.msc
    d. MMC
    e. MSTSC
    f. Notepad
    g. Explorer
    h. Msinfo32
    i. DxDiag
    j. Disk Defragmenter
    k. System Restore
    l. Windows Update

Objective 5 Demonstrate the use of Microsoft Windows Control Panel utilities.

1. Internet Options
    a. Connections
    b. Security

    c. General
    d. Privacy
    e. Programs
    f. Advanced
2. Display/Display Settings
    a. Resolution
    b. Color depth
    c. Refresh rate
3. User Accounts
4. Folder Options
    a. View hidden files
    b. Hide extensions
    c. General options
    d. View options
5. System
    a. Performance (virtual memory)
    b. Remote settings
    c. System protection
6. Windows Firewall
7. Power Options
    a. Hibernate
    b. Power plans
    c. Sleep/suspend
    d. Standby
8. Credential Manager
9. Programs and features
10. HomeGroup
11. Devices and Printers
12. Sound
13. Troubleshooting
14. Network and Sharing Center
15. Device Manager
16. BitLocker
17. Sync Center

Objective 6 Demonstrate Microsoft Windows networking installation on a client/desktop.

1. HomeGroup vs. Workgroup
2. Domain setup
3. Network shares/administrative shares/mapping drives
4. Printer sharing vs. network printer mapping
5. Establish networking connections
    a. VPN
    b. Dial-ups
    c. Wireless
    d. Wired
    e. WWAN (Cellular)
6. Proxy settings
7. Remote Desktop Connection
8. Remote Assistance
9. Home vs. Work vs. Public network settings
10. Firewall settings
    a. Exceptions
    b. Configuration
    c. Enabling/disabling Windows Firewall
11. Configuring an alternative
12. IP address in Windows
    a. IP addressing
    b. Subnet mask
    c. DNS
    d. DHCP
    e. Gateway
13. Network card properties
    a. Half duplex/full duplex/auto
    b. Speed
    c. Wake-on-LAN
    d. QoS
    e. BIOS (on-board NIC)

Objective 7 Demonstrate the use of features and tools of Mac OS and Linux based systems.

1. Best practices
    a. Scheduled backups
    b. Scheduled disk maintenance

c. System updates/App Store
d. Patch management
e. Driver/firmware updates
f. Antivirus/Anti-malware updates

2. Tools
    a. Backup/Time Machine
    b. Restore/Snapshot
    c. Image recovery
    d. Disk maintenance utilities
    e. Shell/Terminal
    f. Screen sharing
    g. Force Quit
3. Features
    a. Multiple desktops/Mission Control
    b. Key Chain

    a. Spot Light
    b. iCloud
    c. Gestures
    d. Finder
    e. Remote Disc
    f. Dock
    g. Boot Camp
2. Basic Linux commands
    a. ls
    b. grep
    c. cd
    d. shutdown
    e. pwd vs. passwd
    f. mv
    g. cp
    h. rm
    i. chmod
    j. chown
    k. iwconfig/ifconfig
    l. ps
    m. su/sudo

n. apt-get
o. vi
p. dd
q. kill

Standard 1 Performance Evaluation included below (Optional)

STANDARD 2

Security

Objective 1 Understand the importance of physical security measures.

1. Mantrap
2. Badge reader
3. Smart card
4. Security guard
5. Door lock
6. Biometric locks
7. Hardware tokens
8. Cable locks
9. Server locks
10. USB locks
11. Privacy screen
12. Key fobs
13. Entry control roster

Objective 2 Understand logical security concepts.

1. Active Directory
    a. Login script
    b. Domain
    c. Group Policy/Updates
    d. Organizational Units
    e. Home Folder
    f. Folder redirection
2. Software tokens
3. MDM policies
4. Port security
5. MAC address filtering

6. Certificates
7. Antivirus/Anti-malware
8. Firewalls
9. User authentication/strong passwords
10. Multifactor authentication
11. Directory permissions
12. VPN
13. DLP
14. Access control lists
15. Smart card
16. Email filtering
17. Trusted/untrusted software sources
18. Principle of least privilege

Objective 3 Understand wireless security protocols and authentication methods.

1. Protocols and encryption
    a. WEP
    b. WPA
    c. WPA2
2. Authentication
    a. Single-factor
    b. Multifactor
    c. RADIUS
    d. TACACS

Objective 4 Demonstrate detection, removal, and prevention of malware using appropriate tools and methods.

1. Malware
    a. Ransomware
    b. Trojan
    c. Keylogger
    d. Rootkit
    e. Virus
    f. Botnet
    g. Worm
    h. Spyware
    i. Adware

j. Rootkits
k. Rogue Security Software

2. Tools and methods
    a. Antivirus
    b. Anti-malware
    c. Recovery console
    d. Backup/restore
    e. End user education
    f. Software firewalls
    g. DNS configuration

Objective 5 Understand social engineering, threats, and vulnerabilities.

1. Social engineering
    a. Phishing
    b. Pharming
    c. Spear phishing
    d. Impersonation
    e. Shoulder surfing
    f. Tailgating
    g. Dumpster diving
2. DDoS
3. DoS
4. Zero-day
5. Man-in-the-middle
6. Brute force
7. Dictionary
8. Rainbow table
9. Spoofing
10. Non-compliant systems
11. Zombie

Objective 6 Understand the basic Microsoft Windows OS security settings.

1. User and groups
    a. Administrator
    b. Power user
    c. Guest
    d. Standard user
2. NTFS vs. share permissions

    a. Allow vs. deny
    b. Moving vs. copying folders and files
    c. File attributes
3. Shared files and folders
    a. Administrative shares vs. local shares
    b. Permission propagation
    c. Inheritance
4. System files and folders
5. User authentication
    a. Single sign-on (SSO)
6. Run as administrator vs. standard user
7. BitLocker
8. BitLocker To Go
9. EFS

Objective 7 Demonstrate best practices in securing devices.

1. Password best practices
    a. Password Entropy and Complexity
    b. Password expiration
    c. Screensaver required password
    d. BIOS/UEFI passwords
    e. Requiring passwords

2. Account management
    a. Restricting user permissions
    b. Logon time restrictions
    c. Disabling guest account
    d. Failed attempts lockout
    e. Timeout/screen lock
    f. Change default admin user account/password
    g. Basic Active Directory functions
        i. Account creation
        ii. Account deletion
        iii. Password reset / unlock account
        iv. Disable account
3. Disable autorun
4. Data encryption
5. Patch/update management
6. Screen locks
    a. o Fingerprint lock
    b. o Face lock
    c. o Swipe lock
    d. o Passcode lock
7. Remote wipes
8. Locator applications
9. Remote backup applications
10. Failed login attempts restrictions
11. Antivirus/Anti-malware
12. Patching/OS updates
13. Biometric authentication
14. Full device encryption
15. Multifactor authentication
16. Authenticator applications
17. Trusted sources vs. untrusted sources
18. Firewalls
19. Policies and procedures
    a. BYOD vs. corporate-owned
    b. Profile security requirements

Objective 8 Understand appropriate data destruction and disposal methods.

1. Physical destruction
    a. Shredder
    b. Drill/hammer
    c. Electromagnetic (Degaussing)
    d. Incineration
    e. Certificate of destruction
2. Recycling or repurposing best practices
    a. Low-level format vs. standard format
    b. Overwrite
    c. Drive wipe

Objective 9 Understand security configuration protocols on networks.

1. Wireless-specific
    a. Changing default SSID
    b. Setting encryption
    c. Disabling SSID broadcast
    d. Antenna and access point placement
    e. Radio power levels (waves)
    f. WPS
2. Change default usernames and passwords
3. Enable MAC filtering
4. Assign static IP addresses
5. Firewall settings
6. Port forwarding/mapping
7. Disabling ports
8. Content filtering/parental controls
9. Update firmware
10. Physical security

Standard 2 Performance Evaluation included below (Optional)

STANDARD 3

Software Troubleshooting

Objective 1 Demonstrate the ability to troubleshoot Microsoft Windows OS problems.

1. Common symptoms
    a. Slow performance

    b. Limited connectivity
    c. Failure to boot
    d. No OS found
    e. Application crashes
    f. Blue screens
    g. Black screens
    h. Printing issues
    i. Services fail to start
    j. Slow bootup
    k. Slow profile load
2. Common solutions
    a. Defragment the hard drive
    b. Reboot
    c. Kill tasks
    d. Restart services
    e. Update network settings
    f. Reimage/reload OS
    g. Roll back updates
    h. Roll back device drivers
    i. Apply updates
    j. Repair application
    k. Update boot order
    l. Disable Windows services/applications
    m. Disable application startup
    n. Safe boot
    o. Rebuild Windows profiles

Objective 2 Understand problems that stem from PC security issues.

1. Common symptoms
    a. Pop-ups
    b. Browser redirection
    c. Security alerts
    d. Slow performance
    e. Internet connectivity issues
    f. PC/OS lockup
    g. Application crash
    h. OS updates failures
    i. Rogue antivirus
    j. Spam
    k. Renamed system files
    l. Disappearing files
    m. File permission changes
    n. Hijacked email
2. Responses from users regarding email
3. Automated replies from unknown sent email
    a. Access denied
    b. Invalid certificate (trusted root CA)
    c. System/application log errors

Objective 3 Understand tools and best practices for malware removal.

1. Identify and research malware symptoms.
2. Quarantine the infected systems.
3. Disable System Restore (in Windows).
4. Remediate the infected systems.
    a. Update the anti-malware software.
    b. Scan and use removal techniques (safe mode, pre-installation environment).
5. Schedule scans and run updates.
6. Enable System Restore and create a restore point (in Windows).
7. Educate the end user.

Standard 3 Performance Evaluation included below (Optional)

STANDARD 4

Operational Procedures

Objective 1 Understand best practices of documenting asset management and enterprise policies.

1. Network topology diagrams
2. Knowledge base/articles
3. Incident documentation
4. Regulatory and compliance policy
5. Acceptable use policy
6. Password policy
7. Inventory management
    a. Asset tags
    b. Barcodes
8. Documented business processes
9. Purpose of the change
10. Scope the change
11. Risk analysis
12. Plan for change
13. End-user acceptance
14. Change board
    a. Approval
15. Backout plan
16. Document changes
17. Incident response
    a. First response
        i. Identify
        ii. Report through proper channels
        iii. Data/device preservation
    b. Use of documentation/ documentation changes
    c. Chain of custody
        i. Tracking of evidence/documenting process
18. Licensing/DRM/EULA
    a. Open-source vs. commercial license
    b. Personal license vs. enterprise licenses
    c. Public domain

    d. Permissive
    e. LGPL
    f. Copyleft
    g. Proprietary
19. Regulated data
    a. PII
    b. PCI
    c. GDPR
    d. PHI
20. Follow all policies and security best practices

Objective 2 Understand safety procedures and environmental concerns.

1. Backup and recovery
    a. Image level
    b. File level
    c. Critical applications
2. Backup testing
3. UPS
4. Surge protector
5. Cloud storage vs. local storage backups
6. Account recovery options
7. Equipment grounding
8. Proper component handling and storage
    a. Antistatic bags
    b. ESD straps
    c. ESD mats
    d. Self-grounding
9. Toxic waste handling
    a. Batteries
    b. Toner
    c. CRT
    d. Cell phones
    e. Tablets
10. Personal safety
    a. Disconnect power before repairing PC
    b. Remove jewelry
    c. Lifting techniques

    d. Weight limitations
    e. Electrical fire safety
    f. Cable management
    g. Safety goggles
    h. Air filter mask
11. MSDS documentation for handling and disposal
12. Temperature, humidity level awareness, and proper ventilation
13. Power surges, brownouts, and blackouts
    a. Battery backup
    b. Surge suppressor
14. Protection from airborne particles
    a. Enclosures
    b. Air filters/mask
15. Dust and debris
    a. Compressed air
    b. Vacuums
16. Compliance with all government regulations

Objective 3 Understand proper communication techniques and professionalism.

1. Use proper language and avoid jargon, acronyms, and slang, when applicable
2. Maintain a positive attitude/ project confidence
3. Actively listen (taking notes) and avoid interrupting the customer
4. Be culturally sensitive
    a. Use appropriate professional titles, when applicable
5. Be on time (if late, contact the customer)
6. Avoid distractions
    a. Personal calls
    b. Texting/social media sites
    c. Talking to coworkers while interacting with customers
    d. Personal interruptions
7. Dealing with difficult customers or situations
    a. Do not argue with customers and/or be defensive
    b. Avoid dismissing customer problems
    c. Avoid being judgmental
    d. Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)
    e. Do not disclose experiences via social media outlets

8. Set and meet expectations/timeline and communicate status with the customer
    a. Offer different repair/ replacement options, if applicable
    b. Provide proper documentation on the services provided
    c. Follow up with customer/user at a later date to verify satisfaction
9. Deal appropriately with customers' confidential and private materials
    a. Located on a computer, desktop, printer, etc

Workplace Skills

1. Communication
2. Problem Solving
3. Teamwork
4. Critical Thinking
5. Dependability
6. Accountability
7. Legal requirements/expectations

Standard 4 Performance Evaluation included below (Optional)

Computer Systems 2

Performance assessments may be completed and evaluated at any time during the course. The following performance skills are to be used in connection with the associated standards and exam. To pass the performance standard the student must attain a performance standard average of 8 or higher on the rating scale. Students may be encouraged to repeat the objectives until they average 8 or higher.

Student's Name: _____

Class: _____

Performance standards rating scale

0	Limited skills	2	→	4	Moderate skills	6	→	8	High skills	10

Standard 1 – Operating Systems **Score:**

- Remote support from an external location.
- Assisting with software, hardware, and operating systems installations, including troubleshooting.

Standard 2 – Security **Score:**

- Ask client/customer various questions about the installed computer systems, run diagnostic, handle software security.

Standard 3 – Software troubleshooting **Score:**

- Highlight customer service and listening skills to understand a customer's problem so that student can help them, even when they are frustrated.

Standard 4 – Operational Procedures **Score:**

- Problem-solving skills are paramount so that you can figure out exactly what is causing the tricky hardware and software issues.

Performance standard average score:

Evaluator Name: _____

Evaluator Title: _____

Evaluator Signature: _____

Date: _____