Cengage

CompTIA A+

Guide to IT Technical Support

Jean Andrews
Joy Dark Shelton
Nicholas Pierce

IT Tech Support

CompTIA A+ Core 1 (220-1011) Exam

	Objective	Modules
Domain 1.0	**Mobile Devices**	
1.1	Given a scenario, install and configure laptop hardware and components	1, 3, 5, 6, 9
1.2	Compare and contrast the display components of mobile devices.	6
1.3	Given a scenario, set up and configure accessories and ports of mobile devices.	1, 9
1.4	Given a scenario, configure basic mobile-device network connectivity and application support.	9
Domain 2.0	**Networking**	
2.1	Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.	7
2.2	Compare and contrast common networking hardware.	7, 8
2.3	Compare and contrast protocols for wireless networking.	8, 9
2.4	Summarize services provided by networked hosts.	7, 8
2.5	Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.	7
2.6	Compare and contrast common network configuration concepts.	7, 8
2.7	Compare and contrast Internet connection types, network types, and their features.	8
2.8	Given a scenario, use networking tools.	8
Domain 3.0	**Hardware**	
3.1	Explain basic cable types and their connectors, features, and purposes.	5, 6, 8
3.2	Given a scenario, install the appropriate RAM.	3
3.3	Given a scenario, select and install storage devices.	5
3.4	Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.	2, 3, 4, 6
3.5	Given a scenario, install or replace the appropriate power supply.	4
3.6	Given a scenario, deploy and configure multifunction devices/printers and settings.	10
3.7	Given a scenario, install and replace printer consumables.	10
Domain 4.0	**Virtualization and Cloud Computing**	
4.1	Summarize cloud-computing concepts.	8
4.2	Summarize aspects of client-side virtualization.	8
Domain 5.0	**Hardware and Network Troubleshooting**	
5.1	Given a scenario, apply the best practice methodology to resolve problems.	4
5.2	Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.	4
5.3	Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.	5
5.4	Given a scenario, troubleshoot video, projector, and display issues.	6
5.5	Given a scenario, troubleshoot common issues with mobile devices.	9
5.6	Given a scenario, troubleshoot and resolve printer issues.	10
5.7	Given a scenario, troubleshoot problems with wired and wireless networks.	8

CompTIA A+ Core 2 (220-1102) Exam

	Objective	Modules
Domain 1.0	**Operating System**	
1.1	Identify basic features of Microsoft Windows editions.	11, 12
1.2	Given a scenario, use the appropriate Microsoft command-line tool.	12, 14, 17, 19
1.3	Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).	12, 13, 14, 16, 17
1.4	Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.	12, 13, 14, 17, 19
1.5	Given a scenario, use the appropriate Windows settings.	12, 13
1.6	Given a scenario, configure Microsoft Windows networking features on a client/desktop.	12, 17, 19
1.7	Given a scenario, apply application installation and configuration concepts.	12
1.8	Explain common OS types and their purposes.	11, 13, 18, 20, 21
1.9	Given a scenario, perform OS installations and upgrades in a diverse OS environment.	11, 12, 15
1.10	Identify common features and tools of the macOS/desktop OS.	20
1.11	Identify common features and tools of the Linux client/desktop OS.	21
Domain 2.0	**Security**	
2.1	Summarize various security measures and their purposes.	16, 17, 18
2.2	Compare and contrast wireless security protocols and authentication methods.	19
2.3	Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.	16
2.4	Explain common social-engineering attacks, threats, and vulnerabilities.	16
2.5	Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.	12, 16, 17, 19
2.6	Given a scenario, configure a workstation to meet best practices for security.	16, 17
2.7	Explain common methods for securing mobile and embedded devices.	18, 19
2.8	Given a scenario, use common data destruction and disposal methods.	16
2.9	Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.	19
2.10	Given a scenario, install and configure browsers and relevant security settings.	19
Domain 3.0	**Software Troubleshooting**	
3.1	Given a scenario, troubleshoot common Windows OS problems.	14, 15
3.2	Given a scenario, troubleshoot common personal computer (PC) security issues.	16
3.3	Given a scenario, use best practice procedures for malware removal.	16
3.4	Given a scenario, troubleshoot common mobile OS and application issues.	18
3.5	Given a scenario, troubleshoot common mobile OS and application security issues.	18
Domain 4.0	**Operational Procedures**	
4.1	Given a scenario, implement best practices associated with documentation and support systems information management.	11, 16
4.2	Explain basic change-management best practices.	11
4.3	Given a scenario, implement workstation backup and recovery methods.	13
4.4	Given a scenario, use common safety procedures.	Appendix A
4.5	Summarize environmental impacts and local environmental controls.	Appendix A
4.6	Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.	16
4.7	Given a scenario, use proper communication techniques and professionalism.	11
4.8	Identify the basics of scripting.	21
4.9	Given a scenario, use remote access technologies.	19, 21

Eleventh Edition

CompTIA A+
Guide to IT Technical Support

Jean Andrews, Ph.D.
Joy Dark Shelton
Nicholas Pierce

IT Tech Support

✢ Cengage

Australia • Brazil • Canada • Mexico • Singapore • United Kingdom • United States

This is an electronic version of the print textbook. Due to electronic rights restrictions, some third party content may be suppressed. Editorial review has deemed that any suppressed content does not materially affect the overall learning experience. The publisher reserves the right to remove content from this title at any time if subsequent rights restrictions require it. For valuable information on pricing, previous editions, changes to current editions, and alternate formats, please visit www.cengage.com/highered to search by ISBN#, author, title, or keyword for materials in your areas of interest.

Important Notice: Media content referenced within the product description or the product text may not be available in the eBook version.

CompTIA A+ Guide To IT Technical Support,
11ᵗʰ edition
Jean Andrews, Joy Dark Shelton, Nicholas Pierce

SVP, Product: Erin Joyner

VP, Product: Thais Alencar

Product Director: Mark Santee

Product Manager: Natalie Onderdonk

Product Assistant: Ethan Wheel

Learning Designer: Carolyn Mako

Senior Content Manager: Brooke Greenhouse

Digital Delivery Quality Partner: Jim Vaughey

Technical Editor: Danielle Shaw

Developmental Editor: Mary Pat Shaffer

VP, Product Marketing: Jason Sakos

Director, Product Marketing: Danaë April

Product Marketing Manager: Mackenzie Paine

IP Analyst: Ann Hoffman

IP Project Manager: Lumina Datamatics

Production Service: Straive

Senior Designer: Erin Griffin

Cover Image Source: Vik Y/Shutterstock.com.

For product information and technology assistance, contact us at
Cengage Customer & Sales Support, 1-800-354-9706
or support.cengage.com.

For permission to use material from this text or product, submit all requests online at **www.copyright.com.**

Cengage is a leading provider of customized learning solutions with employees residing in nearly 40 different countries and sales in more than 125 countries around the world. Find your local representative at **www.cengage.com.**

To learn more about Cengage platforms and services, register or access your online learning solution, or purchase materials for your course, visit **www.cengage.com.**

Notice to the Reader

Publisher does not warrant or guarantee any of the products described herein or perform any independent analysis in connection with any of the product information contained herein. Publisher does not assume, and expressly disclaims, any obligation to obtain and include information other than that provided to it by the manufacturer. The reader is expressly warned to consider and adopt all safety precautions that might be indicated by the activities described herein and to avoid all potential hazards. By following the instructions contained herein, the reader willingly assumes all risks in connection with such instructions. The publisher makes no representations or warranties of any kind, including but not limited to, the warranties of fitness for particular purpose or merchantability, nor are any such representations implied with respect to the material set forth herein, and the publisher takes no responsibility with respect to such material. The publisher shall not be liable for any special, consequential, or exemplary damages resulting, in whole or part, from the readers' use of, or reliance upon, this material.

Contents

Module 6

Supporting I/O Devices   261

Module 7

Networking Fundamentals   309

Module 8

Network Infrastructure and Cloud Computing   363

Module 9

Supporting Mobile Devices   417

Module 10

Supporting Printers   459

Part 2

CompTIA A+ Core 2 (220-1102)   511

Module 14

Troubleshooting Windows After Startup   669

Module 15

Troubleshooting Windows Startup   719

Module 16

Security Strategies   767

Module 17

Module 18

Module 19

Module 20

Supporting macOS   965

Module 21

Linux and Scripting   1005

Appendix A

Safety Procedures and Environmental Concerns

Appendix B

Entry Points for Windows Startup Processes

Appendix C

CompTIA Acronyms

Glossary

Index

CompTIA A+ Core 1 (220-1101) and A+ Core 2 (220-1102) Exam Objectives Mapped to Modules

CompTIA A+ Guide to IT Technical Support, Eleventh Edition fully meets all of the CompTIA's A+ Core 1 (220-1101) and A+ Core 2 (220-1102) Exam Objectives.

CompTIA A+ Core 1 (220-1101)

1.0 Mobile Devices

1.1   Given a scenario, install and configure laptop hardware and components.

Objectives	Primary Module
• Hardware/device replacement	Supporting Processors and Upgrading Memory
▪ Battery	Taking a Computer Apart and Putting It Back Together
▪ Keyboard/keys	Supporting I/O Devices
▪ Random-access memory (RAM)	Supporting Processors and Upgrading Memory
▪ Hard disk drive (HDD)/solid-state drive (SSD) migration	Hard Drives and Other Storage Devices
▪ HDD/SSD replacement	Hard Drives and Other Storage Devices
▪ Wireless cards	Supporting I/O Devices
• Physical privacy and security components	Supporting Mobile Devices
▪ Biometrics	Supporting Mobile Devices
▪ Near-field scanner features	Supporting Mobile Devices

1.2   Compare and contrast the display components of mobile devices.

Objectives	Primary Module
• Types	Supporting I/O Devices
▪ Liquid crystal display (LCD)	Supporting I/O Devices
• In-plane switching (IPS)	Supporting I/O Devices
• Twisted nematic (TN)	Supporting I/O Devices
• Vertical alignment (VA)	Supporting I/O Devices
▪ Organic light-emitting diode (OLED)	Supporting I/O Devices
• Mobile display components	Supporting I/O Devices
• WiFi antenna connector/placement	Supporting I/O Devices
• Camera/webcam	Supporting I/O Devices
• Microphone	Supporting I/O Devices
• Touch screen/digitizer	Supporting I/O Devices
• Inverter	Supporting I/O Devices

1.3   Given a scenario, set up and configure accessories and ports of mobile devices.

Objectives	Primary Module
• Connection methods	Supporting Mobile Devices
▪ Universal Serial Bus (USB)/USB-C/microUSB/ miniUSB	Supporting Mobile Devices
▪ Lightning	Supporting Mobile Devices
▪ Serial interfaces	Supporting Mobile Devices
▪ Near-field communication (NFC)	Supporting Mobile Devices
▪ Bluetooth	Supporting Mobile Devices
▪ Hotspot	Supporting Mobile Devices
• Accessories	Supporting Mobile Devices
▪ Touch pens	Supporting Mobile Devices
▪ Headsets	Supporting Mobile Devices
▪ Speakers	Supporting Mobile Devices
▪ Webcam	Supporting Mobile Devices
• Docking station	Taking a Computer Apart and Putting It Back Together
• Port replicator	Taking a Computer Apart and Putting It Back Together
• Trackpad/drawing pad	Taking a Computer Apart and Putting It Back Together

1.4   Given a scenario, configure basic mobile-device network connectivity and application support.

Objectives	Primary Module
• Wireless/cellular data network (enable/disable)	Supporting Mobile Devices
▪ 2G/3G/4G/5G	Supporting Mobile Devices
▪ Hotspot	Supporting Mobile Devices
▪ Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)	Supporting Mobile Devices
▪ Preferred Roaming List (PRL) updates	Supporting Mobile Devices
• Bluetooth	Supporting Mobile Devices
▪ Enable Bluetooth	Supporting Mobile Devices
▪ Enable pairing	Supporting Mobile Devices
▪ Find a device for pairing	Supporting Mobile Devices
▪ Enter the appropriate PIN code	Supporting Mobile Devices
▪ Test connectivity	Supporting Mobile Devices
• Location services	Supporting Mobile Devices
▪ Global Positioning System (GPS) services	Supporting Mobile Devices
▪ Cellular location services	Supporting Mobile Devices
• Mobile device management (MDM)/mobile application management (MAM)	Supporting Mobile Devices
▪ Corporate email configuration	Supporting Mobile Devices
▪ Two-factor authentication	Supporting Mobile Devices
▪ Corporate applications	Supporting Mobile Devices

Objectives	Primary Module
• Mobile device synchronization	Supporting Mobile Devices
▪ Account setup	Supporting Mobile Devices
• Microsoft 365	Supporting Mobile Devices
• Google Workspace	Supporting Mobile Devices
• iCloud	Supporting Mobile Devices
▪ Data to synchronize	Supporting Mobile Devices
• Mail	Supporting Mobile Devices
• Photos	Supporting Mobile Devices
• Calendar	Supporting Mobile Devices
• Contacts	Supporting Mobile Devices
• Recognizing data caps	Supporting Mobile Devices

2.0 Networking

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

Objectives	Primary Module
• Ports and protocols	Networking Fundamentals
▪ 20/21 – File Transfer Protocol (FTP)	Networking Fundamentals
▪ 22 – Secure Shell (SSH)	Networking Fundamentals
▪ 23 – Telnet	Networking Fundamentals
▪ 25 – Simple Mail Transfer Protocol (SMTP)	Networking Fundamentals
▪ 53 – Domain Name System (DNS)	Networking Fundamentals
▪ 67/68 – Dynamic Host Configuration Protocol (DHCP)	Networking Fundamentals
▪ 80 – Hypertext Transfer Protocol (HTTP)	Networking Fundamentals
▪ 110 – Post Office Protocol 3 (POP3)	Networking Fundamentals
▪ 137/139 – Network Basic Input/Output System (NetBIOS)/ NetBIOS over TCP/IP (NetBT)	Networking Fundamentals
▪ 143 – Internet Mail Access Protocol (IMAP)	Networking Fundamentals
▪ 161/162 – Simple Network Management Protocol (SNMP)	Networking Fundamentals
▪ 389 – Lightweight Directory Access Protocol (LDAP)	Networking Fundamentals
▪ 443 – Hypertext Transfer Protocol Secure (HTTPS)	Networking Fundamentals
▪ 445 – Server Message Block (SMB)/Common Internet File System (CIFS)	Networking Fundamentals
▪ 3389 – Remote Desktop Protocol (RDP)	Networking Fundamentals
• TCP vs. UDP	Networking Fundamentals
▪ Connectionless	Networking Fundamentals
• DHCP	Networking Fundamentals
• Trivia File Transfer Protocol (TFTP)	Networking Fundamentals
▪ Connection-oriented	Networking Fundamentals
• HTTPS	Networking Fundamentals
• SSH	Networking Fundamentals

2.2   Compare and contrast common networking hardware.

Objectives	Primary Module
• Routers	Networking Fundamentals
• Switches	Networking Fundamentals
▪ Managed	Network Infrastructure and Cloud Computing
▪ Unmanaged	Network Infrastructure and Cloud Computing
• Access points	Network Infrastructure and Cloud Computing
• Patch panel	Network Infrastructure and Cloud Computing
• Firewall	Network Infrastructure and Cloud Computing
• Power over Ethernet (PoE)	Network Infrastructure and Cloud Computing
▪ Injectors	Network Infrastructure and Cloud Computing
▪ Switch	Network Infrastructure and Cloud Computing
▪ PoE standards	Network Infrastructure and Cloud Computing
• Hub	Networking Fundamentals
• Cable modem	Networking Fundamentals
• Digital subscriber line (DSL)	Network Infrastructure and Cloud Computing
• Optical network terminal (ONT)	Network Infrastructure and Cloud Computing
• Network interface card (NIC)	Networking Fundamentals
• Software-defined networking (SDN)	Network Infrastructure and Cloud Computing

2.3   Compare and contrast protocols for wireless networking.

Objectives	Primary Module
• Frequencies	Network Infrastructure and Cloud Computing
▪ 2.4GHz	Network Infrastructure and Cloud Computing
▪ 5GHz	Network Infrastructure and Cloud Computing
• Channels	Network Infrastructure and Cloud Computing
▪ Regulations	Network Infrastructure and Cloud Computing
▪ 2.4GHz vs. 5GHz	Network Infrastructure and Cloud Computing
• Bluetooth	Supporting Mobile Devices
• 802.11	Network Infrastructure and Cloud Computing
▪ a	Network Infrastructure and Cloud Computing
▪ b	Network Infrastructure and Cloud Computing
▪ g	Network Infrastructure and Cloud Computing
▪ n	Network Infrastructure and Cloud Computing
▪ ac (WiFi 5)	Network Infrastructure and Cloud Computing
▪ ax (WiFi 6)	Network Infrastructure and Cloud Computing
• Long-range fixed wireless	Network Infrastructure and Cloud Computing
▪ Licensed	Network Infrastructure and Cloud Computing
▪ Unlicensed	Network Infrastructure and Cloud Computing

Objectives	Primary Module
▪ Power	Network Infrastructure and Cloud Computing
▪ Regulatory requirements for wireless power	Network Infrastructure and Cloud Computing
• NFC	Supporting Mobile Devices
• Radio-frequency identification (RFID)	Supporting Mobile Devices

2.4   Summarize services provided by networked hosts.

Objectives	Primary Module
• Server roles	Networking Fundamentals
▪ DNS	Networking Fundamentals
▪ DHCP	Networking Fundamentals
▪ Fileshare	Networking Fundamentals
▪ Print servers	Networking Fundamentals
▪ Mail servers	Networking Fundamentals
▪ Syslog	Networking Fundamentals
▪ Web servers	Networking Fundamentals
▪ Authentication, authorization, and accounting (AAA)	Networking Fundamentals
• Internet appliances	Network Infrastructure and Cloud Computing
▪ Spam gateways	Network Infrastructure and Cloud Computing
▪ Unified threat management (UTM)	Network Infrastructure and Cloud Computing
▪ Load balancers	Network Infrastructure and Cloud Computing
▪ Proxy servers	Networking Fundamentals
• Legacy/embedded systems	Network Infrastructure and Cloud Computing
▪ Supervisory control and data acquisition (SCADA)	Network Infrastructure and Cloud Computing
• Internet of Things (IoT) devices	Network Infrastructure and Cloud Computing

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

Objectives	Primary Module
• Internet Protocol (IP) addressing	Networking Fundamentals
▪ IPv4	Networking Fundamentals
• Private addresses	Networking Fundamentals
• Public addresses	Networking Fundamentals
▪ IPv6	Networking Fundamentals
▪ Automatic Private IP Addressing (APIPA)	Networking Fundamentals
▪ Static	Networking Fundamentals
▪ Dynamic	Networking Fundamentals
▪ Gateway	Networking Fundamentals

2.6   Compare and contrast common network configuration concepts.

Objectives	Primary Module
• DNS	Networking Fundamentals
▪ Address (A)	Networking Fundamentals
▪ Address (AAAA)	Networking Fundamentals
▪ Mail exchanger (MX)	Networking Fundamentals
▪ Text (TXT)	Networking Fundamentals
• Spam management	Networking Fundamentals
(i) DomainKeys Identified Mail (DKIM)	Networking Fundamentals
(ii) Sender Policy Framework (SPF)	Networking Fundamentals
(iii) Domain-based Message Authentication, Reporting, and Conformance (DMARC)	Networking Fundamentals
• DHCP	Networking Fundamentals
▪ Leases	Networking Fundamentals
▪ Reservations	Networking Fundamentals
▪ Scope	Networking Fundamentals
• Virtual LAN (VLAN)	Network Infrastructure and Cloud Computing
• Virtual private network (VPN)	Network Infrastructure and Cloud Computing

2.7   Compare and contrast Internet connection types, network types, and their features.

Objectives	Primary Module
• Internet connection types	Network Infrastructure and Cloud Computing
▪ Satellite	Network Infrastructure and Cloud Computing
▪ Fiber	Network Infrastructure and Cloud Computing
▪ Cable	Network Infrastructure and Cloud Computing
▪ DSL	Network Infrastructure and Cloud Computing
▪ Cellular	Network Infrastructure and Cloud Computing
▪ Wireless Internet service provider (WISP)	Network Infrastructure and Cloud Computing
• Network types	Network Infrastructure and Cloud Computing
▪ Local area network (LAN)	Network Infrastructure and Cloud Computing
▪ Wide area network (WAN)	Network Infrastructure and Cloud Computing
▪ Personal area network (PAN)	Network Infrastructure and Cloud Computing
▪ Metropolitan area network (MAN)	Network Infrastructure and Cloud Computing
▪ Storage area network (SAN)	Network Infrastructure and Cloud Computing
▪ Wireless local area network (WLAN)	Network Infrastructure and Cloud Computing

2.8 Given a scenario, use networking tools.

Objectives	Primary Module
• Crimper	Network Infrastructure and Cloud Computing
• Cable stripper	Network Infrastructure and Cloud Computing

Objectives	Primary Module
• WiFi analyzer	Network Infrastructure and Cloud Computing
• Toner probe	Network Infrastructure and Cloud Computing
• Punchdown tool	Network Infrastructure and Cloud Computing
• Cable tester	Network Infrastructure and Cloud Computing
• Loopback plug	Network Infrastructure and Cloud Computing
• Network tap	Network Infrastructure and Cloud Computing

3.0 Hardware

3.1   Explain basic cable types and their connectors, features, and purposes.

Objectives	Primary Module
• Network cables	Network Infrastructure and Cloud Computing
▪ Copper	Network Infrastructure and Cloud Computing
• Cat 5	Network Infrastructure and Cloud Computing
• Cat 5e	Network Infrastructure and Cloud Computing
• Cat 6	Network Infrastructure and Cloud Computing
• Cat 6a	Network Infrastructure and Cloud Computing
• Coaxial	Network Infrastructure and Cloud Computing
• Shielded twisted pair	Network Infrastructure and Cloud Computing
(i) Direct burial	Network Infrastructure and Cloud Computing
• Unshielded twisted pair	Network Infrastructure and Cloud Computing
▪ Plenum	Network Infrastructure and Cloud Computing
▪ Optical	Network Infrastructure and Cloud Computing
• Fiber	Network Infrastructure and Cloud Computing
▪ T568A/T568B	Network Infrastructure and Cloud Computing
• Peripheral cables	Supporting I/O Devices
▪ USB 2.0	Supporting I/O Devices
▪ USB 3.0	Supporting I/O Devices
▪ Serial	Supporting I/O Devices
▪ Thunderbolt	Supporting I/O Devices
• Video cables	Supporting I/O Devices
▪ High-Definition Multimedia Interface (HDMI)	Supporting I/O Devices
▪ DisplayPort	Supporting I/O Devices
▪ Digital Visual Interface (DVI)	Supporting I/O Devices
▪ Video Graphics Array (VGA)	Supporting I/O Devices
• Hard drive cables	Hard Drives and Other Storage Devices
▪ Serial Advanced Technology Attachment (SATA)	Hard Drives and Other Storage Devices
▪ Small Computer System Interface (SCSI)	Hard Drives and Other Storage Devices
▪ External SATA (eSATA)	Hard Drives and Other Storage Devices
▪ Integrated Drive Electronics (IDE)	Hard Drives and Other Storage Devices

Objectives	Primary Module
• Adapters	Supporting I/O Devices
• Connector types	
▪ RJ11	Network Infrastructure and Cloud Computing
▪ RJ45	Network Infrastructure and Cloud Computing
▪ F type	Network Infrastructure and Cloud Computing
▪ Straight tip (ST)	Network Infrastructure and Cloud Computing
▪ Subscriber connector (SC)	Network Infrastructure and Cloud Computing
▪ Lucent connector (LC)	Network Infrastructure and Cloud Computing
▪ Punchdown block	Network Infrastructure and Cloud Computing
▪ microUSB	Supporting I/O Devices
▪ miniUSB	Supporting I/O Devices
▪ USB-C	Supporting I/O Devices
▪ Molex	All About Motherboards
▪ Lightning port	Supporting I/O Devices
▪ DB9	Supporting I/O Devices

3.2   Given a scenario, install the appropriate RAM.

Objectives	Primary Module
• RAM types	Supporting Processors and Upgrading Memory
▪ Virtual RAM	Supporting Processors and Upgrading Memory
▪ Small outline dual inline memory module (SODIMM)	Supporting Processors and Upgrading Memory
▪ Double Data Rate 3 (DDR3)	Supporting Processors and Upgrading Memory
▪ Double Data Rate 4 (DDR4)	Supporting Processors and Upgrading Memory
▪ Double Data Rate 5 (DDR5)	Supporting Processors and Upgrading Memory
▪ Error correction code (ECC) RAM	Supporting Processors and Upgrading Memory
• Single-channel	Supporting Processors and Upgrading Memory
• Dual-channel	Supporting Processors and Upgrading Memory
• Triple-channel	Supporting Processors and Upgrading Memory
• Quad-channel	Supporting Processors and Upgrading Memory

3.3   Given a scenario, select and install storage devices.

Objectives	Primary Module
• Hard drives	Hard Drives and Other Storage Devices
▪ Speeds	Hard Drives and Other Storage Devices
• 5,400rpm	Hard Drives and Other Storage Devices
• 7,200rpm	Hard Drives and Other Storage Devices
• 10,000rpm	Hard Drives and Other Storage Devices
• 15,000rpm	Hard Drives and Other Storage Devices

Objectives	Primary Module
▪ Form factor	Hard Drives and Other Storage Devices
• 2.5	Hard Drives and Other Storage Devices
• 3.5	Hard Drives and Other Storage Devices
• SSDs	Hard Drives and Other Storage Devices
▪ Communications interfaces	Hard Drives and Other Storage Devices
• Non-volatile Memory Express (NVMe)	Hard Drives and Other Storage Devices
• SATA	Hard Drives and Other Storage Devices
• Peripheral Component Interconnect Express (PCIe)	Hard Drives and Other Storage Devices
▪ Form factors	Hard Drives and Other Storage Devices
• M.2	Hard Drives and Other Storage Devices
• mSATA	Hard Drives and Other Storage Devices
• Drive configurations	Hard Drives and Other Storage Devices
▪ Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10	Hard Drives and Other Storage Devices
• Removable storage	Hard Drives and Other Storage Devices
▪ Flash drives	Hard Drives and Other Storage Devices
▪ Memory cards	Hard Drives and Other Storage Devices
▪ Optical drives	Hard Drives and Other Storage Devices

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

Objectives	Primary Module
• Motherboard form factor	All About Motherboards
▪ Advanced Technology eXtended (ATX)	All About Motherboards
▪ Information Technology eXtended (ITX)	All About Motherboards
• Motherboard connector types	All About Motherboards
▪ Peripheral Component Interconnect (PCI)	All About Motherboards
▪ PCI Express (PCIe)	All About Motherboards
▪ Power connectors	All About Motherboards
▪ SATA	All About Motherboards
▪ eSATA	All About Motherboards
▪ Headers	All About Motherboards
▪ M.2	All About Motherboards
• Motherboard compatibility	Supporting Processors and Upgrading Memory
▪ CPU sockets	Supporting Processors and Upgrading Memory
• Advanced Micro Devices, Inc. (AMD)	Supporting Processors and Upgrading Memory
• Intel	Supporting Processors and Upgrading Memory

Objectives	Primary Module
▪ Server	Supporting Processors and Upgrading Memory
▪ Multisocket	Supporting Processors and Upgrading Memory
▪ Desktop	All About Motherboards
▪ Mobile	All About Motherboards
• Basic Input/Output System (BIOS)/Unified Extensible Firmware Interface (UEFI) settings	All About Motherboards
▪ Boot options	All About Motherboards
▪ USB permissions	All About Motherboards
▪ Trusted Platform Module (TPM) security features	All About Motherboards
▪ Fan considerations	All About Motherboards
▪ Secure Boot	All About Motherboards
▪ Boot password	All About Motherboards
• Encryption	All About Motherboards
▪ TPM	All About Motherboards
▪ Hardware security module (HSM)	All About Motherboards
• CPU architecture	Supporting Processors and Upgrading Memory
▪ x64/x86	Supporting Processors and Upgrading Memory
▪ Advanced RISC Machine (ARM)	Supporting Processors and Upgrading Memory
▪ Single-core	Supporting Processors and Upgrading Memory
▪ Multicore	Supporting Processors and Upgrading Memory
▪ Multithreading	Supporting Processors and Upgrading Memory
▪ Virtualization support	Supporting Processors and Upgrading Memory
• Expansion cards	Supporting I/O Devices
▪ Sound card	Supporting I/O Devices
▪ Video card	Supporting I/O Devices
▪ Capture card	Supporting I/O Devices
▪ NIC	Supporting I/O Devices
• Cooling	Power Supplies and Troubleshooting Computer Problems
▪ Fans	Power Supplies and Troubleshooting Computer Problems
▪ Heat sink	Power Supplies and Troubleshooting Computer Problems
▪ Thermal paste/pads	Power Supplies and Troubleshooting Computer Problems
▪ Liquid	Power Supplies and Troubleshooting Computer Problems

3.5   Given a scenario, install or replace the appropriate power supply.

Objectives	Primary Module
• Input 110–120 VAC vs. 220–240 VAC	Power Supplies and Troubleshooting Computer Problems
• Output 3.3V vs. 5V vs. 12V	Power Supplies and Troubleshooting Computer Problems
• 20-pin to 24-pin motherboard adapter	Power Supplies and Troubleshooting Computer Problems

Objectives	Primary Module
• Redundant power supply	Power Supplies and Troubleshooting Computer Problems
• Modular power supply	Power Supplies and Troubleshooting Computer Problems
• Wattage rating	Power Supplies and Troubleshooting Computer Problems

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

Objectives	Primary Module
• Properly unboxing a device – setup location considerations	Supporting Printers
• Use appropriate drivers for a given OS	Supporting Printers
▪ Printer Control Language (PCL) vs. PostScript	Supporting Printers
• Device connectivity	Supporting Printers
▪ USB	Supporting Printers
▪ Ethernet	Supporting Printers
▪ Wireless	Supporting Printers
• Public/shared devices	Supporting Printers
▪ Printer share	Supporting Printers
▪ Print server	Supporting Printers
• Configuration settings	Supporting Printers
▪ Duplex	Supporting Printers
▪ Orientation	Supporting Printers
▪ Tray settings	Supporting Printers
▪ Quality	Supporting Printers
• Security	Supporting Printers
▪ User authentication	Supporting Printers
▪ Badging	Supporting Printers
▪ Audit logs	Supporting Printers
▪ Secured prints	Supporting Printers
• Network scan services	Supporting Printers
▪ Email	Supporting Printers
▪ SMB	Supporting Printers
▪ Cloud services	Supporting Printers
• Automatic document feeder (ADF)/flatbed scanner	Supporting Printers

3.7   Given a scenario, install and replace printer consumables.

Objectives	Primary Module
• Laser	Supporting Printers
▪ Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, duplexing assembly	Supporting Printers
▪ Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning	Supporting Printers
▪ Maintenance: Replace toner, apply maintenance kit, calibrate, clean	Supporting Printers
• Inkjet	Supporting Printers
▪ Ink cartridge, print head, roller, feeder, duplexing assembly, carriage belt	Supporting Printers
▪ Calibration	Supporting Printers
▪ Maintenance: Clean heads, replace cartridges, calibrate, clear jams	Supporting Printers
• Thermal	Supporting Printers
▪ Feed assembly, heating element	Supporting Printers
▪ Special thermal paper	Supporting Printers
▪ Maintenance: Replace paper, clean heating element, remove debris	Supporting Printers
▪ Heat sensitivity of paper	Supporting Printers
• Impact	Supporting Printers
▪ Print head, ribbon, tractor feed	Supporting Printers
▪ Impact paper	Supporting Printers
▪ Maintenance: Replace ribbon, replace print head, replace paper	Supporting Printers
• 3-D printer	Supporting Printers
▪ Filament	Supporting Printers
▪ Resin	Supporting Printers
▪ Print bed	Supporting Printers

4.0 Virtualization and Cloud Computing

4.1   Summarize cloud-computing concepts.

Objectives	Primary Module
• Common cloud models	Network Infrastructure and Cloud Computing
▪ Private cloud	Network Infrastructure and Cloud Computing
▪ Public cloud	Network Infrastructure and Cloud Computing
▪ Hybrid cloud	Network Infrastructure and Cloud Computing
▪ Community cloud	Network Infrastructure and Cloud Computing
▪ Infrastructure as a service (IaaS)	Network Infrastructure and Cloud Computing
▪ Software as a service (SaaS)	Network Infrastructure and Cloud Computing
▪ Platform as a service (PaaS)	Network Infrastructure and Cloud Computing
• Cloud characteristics	Network Infrastructure and Cloud Computing
▪ Shared resources	Network Infrastructure and Cloud Computing
▪ Metered utilization	Network Infrastructure and Cloud Computing

Objectives	Primary Module
▪ Rapid elasticity	Network Infrastructure and Cloud Computing
▪ High availability	Network Infrastructure and Cloud Computing
▪ File synchronization	Network Infrastructure and Cloud Computing
• Desktop virtualization	Network Infrastructure and Cloud Computing
▪ Virtual desktop infrastructure (VDI) on premises	Network Infrastructure and Cloud Computing
▪ VDI in the cloud	Network Infrastructure and Cloud Computing

4.2 Summarize aspects of client-side virtualization.

Objectives	Primary Module
• Purpose of virtual machines	Network Infrastructure and Cloud Computing
▪ Sandbox	Network Infrastructure and Cloud Computing
▪ Test development	Network Infrastructure and Cloud Computing
▪ Application virtualization	Network Infrastructure and Cloud Computing
• Legacy software/OS	Network Infrastructure and Cloud Computing
• Cross-platform virtualization	Network Infrastructure and Cloud Computing
• Resource requirements	Network Infrastructure and Cloud Computing
• Security requirements	Network Infrastructure and Cloud Computing

5.0 Hardware and Network Troubleshooting

5.1 Given a scenario, apply the best practice methodology to resolve problems.

Objectives	Primary Module
• Always consider corporate policies, procedures, and impacts before implementing changes	Power Supplies and Troubleshooting Computer Problems
1. Identify the problem	Power Supplies and Troubleshooting Computer Problems
• Gather information from the user, identify user changes, and, if applicable, perform backups before making changes	Power Supplies and Troubleshooting Computer Problems
• Inquire regarding environmental or infrastructure changes	Power Supplies and Troubleshooting Computer Problems
2. Establish a theory of probable cause (question the obvious)	Power Supplies and Troubleshooting Computer Problems
• If necessary, conduct external or internal research based on symptoms	Power Supplies and Troubleshooting Computer Problems
3. Test the theory to determine the cause	Power Supplies and Troubleshooting Computer Problems
• Once the theory is confirmed, determine the next steps to resolve the problem	Power Supplies and Troubleshooting Computer Problems
• If the theory is not confirmed, re-establish a new theory or escalate	Power Supplies and Troubleshooting Computer Problems

Objectives	Primary Module
4. Establish a plan of action to resolve the problem and implement the solution	Power Supplies and Troubleshooting Computer Problems
• Refer to the vendor's instructions for guidance	Power Supplies and Troubleshooting Computer Problems
5. Verify full system functionality and, if applicable, implement preventive measures	Power Supplies and Troubleshooting Computer Problems
6. Document the findings, actions, and outcomes	Power Supplies and Troubleshooting Computer Problems

5.2   Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.

Objectives	Primary Module
• Common symptoms	Power Supplies and Troubleshooting Computer Problems
▪ Power-on self-test (POST) beeps	Power Supplies and Troubleshooting Computer Problems
▪ Proprietary crash screens (blue screen of death [BSOD]/pinwheel)	Power Supplies and Troubleshooting Computer Problems
▪ Black screen	Power Supplies and Troubleshooting Computer Problems
▪ No power	Power Supplies and Troubleshooting Computer Problems
▪ Sluggish performance	Power Supplies and Troubleshooting Computer Problems
▪ Overheating	Power Supplies and Troubleshooting Computer Problems
▪ Burning smell	Power Supplies and Troubleshooting Computer Problems
▪ Intermittent shutdown	Power Supplies and Troubleshooting Computer Problems
▪ Application crashes	Power Supplies and Troubleshooting Computer Problems
▪ Grinding noise	Power Supplies and Troubleshooting Computer Problems
▪ Capacitor swelling	Power Supplies and Troubleshooting Computer Problems
▪ Inaccurate system date/time	Power Supplies and Troubleshooting Computer Problems

5.3 Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.

Objectives	Primary Module
• Common symptoms	Hard Drives and Other Storage Devices
▪ Light-emitting diode (LED) status indicators	Hard Drives and Other Storage Devices
▪ Grinding noises	Hard Drives and Other Storage Devices
▪ Clicking sounds	Hard Drives and Other Storage Devices
▪ Bootable device not found	Hard Drives and Other Storage Devices
▪ Data loss/corruption	Hard Drives and Other Storage Devices
▪ RAID failure	Hard Drives and Other Storage Devices
▪ Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T.) failure	Hard Drives and Other Storage Devices
▪ Extended read/write times	Hard Drives and Other Storage Devices
▪ Input/output operations per second (IOPS)	Hard Drives and Other Storage Devices
▪ Missing drives in OS	Hard Drives and Other Storage Devices

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

Objectives	Primary Module
• Common symptoms	Supporting I/O Devices
▪ Incorrect data source	Supporting I/O Devices
▪ Physical cabling issues	Supporting I/O Devices
▪ Burned-out bulb	Supporting I/O Devices
▪ Fuzzy image	Supporting I/O Devices
▪ Display burn-in	Supporting I/O Devices
▪ Dead pixels	Supporting I/O Devices
▪ Flashing screen	Supporting I/O Devices
▪ Incorrect color display	Supporting I/O Devices
▪ Audio issues	Supporting I/O Devices
▪ Dim image	Supporting I/O Devices
▪ Intermittent projector shutdown	Supporting I/O Devices

5.5   Given a scenario, troubleshoot common issues with mobile devices.

Objectives	Primary Module
• Common symptoms	Supporting Mobile Devices
▪ Poor battery health	Supporting Mobile Devices
▪ Swollen battery	Supporting Mobile Devices
▪ Broken screen	Supporting Mobile Devices
▪ Improper charging	Supporting Mobile Devices
▪ Poor/no connectivity	Supporting Mobile Devices
▪ Liquid damage	Supporting Mobile Devices
▪ Overheating	Supporting Mobile Devices
▪ Digitizer issues	Supporting Mobile Devices
▪ Physically damaged ports	Supporting Mobile Devices
▪ Malware	Supporting Mobile Devices
▪ Cursor drift/touch calibration	Supporting Mobile Devices

5.6   Given a scenario, troubleshoot and resolve printer issues.

Objectives	Primary Module
• Common symptoms	Supporting Printers
▪ Lines down the printed pages	Supporting Printers
▪ Garbled print	Supporting Printers
▪ Toner not fusing to paper	Supporting Printers
▪ Paper jams	Supporting Printers
▪ Faded print	Supporting Printers
▪ Incorrect paper size	Supporting Printers
▪ Paper not feeding	Supporting Printers

Objectives	Primary Module
▪ Multipage misfeed	Supporting Printers
▪ Multiple prints pending in queue	Supporting Printers
▪ Speckling on printed pages	Supporting Printers
▪ Double/echo images on the print	Supporting Printers
▪ Incorrect color display	Supporting Printers
▪ Grinding noise	Supporting Printers
▪ Finishing issues	Supporting Printers
• Staple jams	Supporting Printers
• Hole punch	Supporting Printers
▪ Incorrect page orientation	Supporting Printers

5.7   Given a scenario, troubleshoot problems with wired and wireless networks.

Objectives	Primary Module
• Common symptoms	Network Infrastructure and Cloud Computing
▪ Intermittent wireless connectivity	Network Infrastructure and Cloud Computing
▪ Slow network speeds	Network Infrastructure and Cloud Computing
▪ Limited connectivity	Network Infrastructure and Cloud Computing
▪ Jitter	Network Infrastructure and Cloud Computing
▪ Poor Voice over Internet Protocol (VoIP) quality	Network Infrastructure and Cloud Computing
▪ Port flapping	Network Infrastructure and Cloud Computing
▪ High latency	Network Infrastructure and Cloud Computing
▪ External interference	Network Infrastructure and Cloud Computing

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
▪ Desktop styles/user interface	Installing Windows

Objectives	Primary Module
▪ 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
▪ 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
▪ 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
▪ 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
▪ 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
▪ 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
▪ 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
• 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

Objectives	Primary Module
• File Explorer Options	Maintaining Windows
▪ Show hidden files	Maintaining Windows
▪ Hide extensions	Maintaining Windows
▪ General options	Maintaining Windows
▪ View options	Maintaining Windows
• 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
• 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
▪ 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
▪ 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
▪ 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
▪ 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
• 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

Objectives	Primary Module
▪ Other considerations	Installing Windows
• Third-party drivers	The Complex World of IT Professionals
• Partitioning	The Complex World of IT Professionals
▪ 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
▪ 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
▪ Mission Control	Supporting macOS

Objectives	Primary Module
▪ 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
• 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
▪ 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
▪ 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

Objectives	Primary Module
• 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
▪ 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
▪ 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

Objectives	Primary Module
• Mobile device management (MDM)	Mobile Device Security
• Active Directory	Securing and Sharing Windows Resources
▪ Login script	Securing and Sharing Windows Resources
▪ 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
▪ 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
▪ Boot sector virus	Security Strategies
▪ Cryptominers	Security Strategies
• Tools and methods	Security Strategies
▪ Recovery console	Security Strategies
▪ Antivirus	Security Strategies
▪ Anti-malware	Security Strategies

Objectives	Primary Module
▪ 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
▪ 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
▪ 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

Objectives	Primary Module
• Firewall	Network Security and Troubleshooting
▪ Activate/deactivate	Network Security and 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
▪ 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
• 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
▪ 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
• 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
• 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

Objectives	Primary Module
• 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
▪ 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
▪ 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
▪ 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

Objectives	Primary Module
• Password managers	Network Security and Troubleshooting
• 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
▪ 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
▪ 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
▪ 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
• 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
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
▪ 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

Objectives	Primary Module
▪ 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
▪ 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 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

Objectives	Primary Module
• Progress notes	The Complex World of IT 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 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
▪ 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
• 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
▪ 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
▪ 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
• 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
▪ 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
• 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

Objectives	Primary Module
• 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
▪ 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 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 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

Objectives	Primary Module
• 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, restate the issue, or question to verify understanding)	The Complex World of IT Professionals
▪ 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
▪ 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
▪ 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
▪ 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
• Security considerations of each access method	Network Security and Troubleshooting

Introduction: CompTIA A+ Guide to IT Technical Support

CompTIA A+ Guide to IT Technical Support, Eleventh Edition was written to be the very best tool on the market today to prepare you to support users and their resources on networks, desktops, laptops, mobile devices, virtual machines, and in the cloud. This edition has been updated to include the most current hardware and software technologies; this text takes you from the just-a-user level to the I-can-fix-this level for hardware, software, networks, and virtual computing infrastructures. It achieves its goals with an unusually effective combination of tools that powerfully reinforce both concepts and hands-on, real-world experiences. It also provides thorough preparation for the content on the new CompTIA A+ Core 1 and Core 2 Certification exams. Competency in using a computer is a prerequisite to using this text. No background knowledge of electronics or networking is assumed. An appropriate prerequisite course for this text would be a general course in computer applications.

This text includes:

- **Several in-depth, hands-on projects** at the end of each module that invite you to immediately apply and reinforce critical thinking and troubleshooting skills and are designed to make certain that you not only understand the material but also execute procedures and make decisions on your own.
- **Comprehensive review and practice end-of-module material**, including a module summary, key terms list, critical thinking questions that focus on the type of scenarios you might expect on A+ exam questions, and real-world problems to solve.
- **Step-by-step instructions** on installation, maintenance, optimization of system performance, and troubleshooting.
- **A wide array of photos, drawings, and screenshots** support the text, displaying in detail the exact software and hardware features you will need to understand to set up, maintain, and troubleshoot physical and virtual computers and small networks.

In addition, the carefully structured, clearly written text is accompanied by graphics that provide the visual input essential to learning and to help students master difficult subject matter. For instructors using the text in a classroom, instructor resources are available online.

Coverage is balanced—while focusing on new technologies and software, including virtualization, cloud computing, the Internet of Things, and Windows 10/11, the text also covers the real world of an IT support technician, where some older technologies remain in widespread use and still need support. For example, the text covers M.2 motherboard slots and NVMe, the latest drive interface standard for solid-state devices (SSDs), but also addresses how to install SSDs and magnetic hard drives using the older Serial Advanced Technology Attachment (SATA) interfaces. The text focuses on Windows 10, the most popular operating system for desktops and laptops, but also covers

Windows 11, macOS, Linux, and Chrome OS for desktops and Android and iOS for mobile devices. Other covered content that is new with the latest A+ Core 1 and Core 2 exams includes enhanced coverage for Domain Name Service (DNS), security and backup techniques, software troubleshooting, macOS, Linux, and scripting.

This text provides thorough preparation for CompTIA's A+ Core 1 and Core 2 Certification examinations. This certification credential's popularity among employers is growing exponentially, and obtaining certification increases your ability to gain employment and improve your salary. To get more information on CompTIA's A+ certification and its sponsoring organization, the Computing Technology Industry Association, see their website at *www.comptia.org*.

Features

To ensure a successful learning experience, this text includes the following pedagogical features:

- **A Clean Split Between Core 1 and Core 2.** The first 10 modules focus on content on the A+ Core 1 exam, while the remaining 11 modules and an appendix focus on the A+ Core 2 exam. The appendix "Safety Procedures and Environmental Concerns," covered on the Core 2 exam, is set apart from Core 2 modules as an appendix to make it easier for students studying modules about hardware to find this content, which is so important to protecting yourself, the hardware, and the environment.
- **Learning Objectives.** Every module opens with lists of learning objectives and A+ certification objectives that set the stage for you to absorb the lessons of the text.
- **Comprehensive Step-by-Step Troubleshooting Guidance.** Troubleshooting guidelines are included in almost every module. In addition, the Core 1 module "Power Supplies and Troubleshooting Computer Problems" gives insights into general approaches to troubleshooting that help apply the specifics detailed in each module for different hardware and software problems. Several Core 2 modules focus on troubleshooting networks, applications, and Windows.
- **Step-by-Step Procedures.** The text is chock-full of step-by-step procedures covering subjects from hardware and operating system installations and maintenance to troubleshooting the boot process or a failed network connection and optimizing system performance.
- **Visual Learning.** Numerous visually detailed photographs, three-dimensional art, and screenshots support the text, displaying hardware and software features exactly as you will see them in your work.
- **CompTIA A+ Objectives Mapped to Modules.** This table lists the module that provides the primary content for each certification objective on the A+ exams. This is a valuable tool for quick reference.
- **Applying Concepts.** These sections offer real-life, practical applications for the material being discussed. Whether outlining a task, developing a scenario, or providing pointers, the Applying Concepts sections give you a chance to apply what you've learned to a typical computer or network problem, so you can understand how you will use the material in your professional life.
- **Page edge colors distinguish Core 1 modules from Core 2 modules.** To help you keep track of which exam is covered by each module, the pages of modules with Core 1 content are edged in teal while the Core 2 modules are edged in orange. Although not essential, it is suggested that you cover the Core 1 modules before you complete the Core 2 modules. This suggestion especially applies to the modules on networking.

Core 1 Objective
Core 2 Objective
Notes
Exam Tip ✔
Caution ❗
Core to Core ↔

- **Exam Objectives.** The relevant exam objective numbers are included for all content that relates to CompTIA's A+ Core 1 and A+ Core 2 Certification exams. This unique feature highlights the relevant content at a glance, so that you can pay extra attention to the material.
- **Notes.** Numbered Note boxes highlight additional helpful information related to the subject being discussed.
- **Exam Tip Boxes.** These boxes highlight additional insights and tips to remember if you are planning to take the CompTIA A+ exams.
- **Caution Boxes.** These icons highlight critical safety information. Follow these instructions carefully to protect the computer and its data and to ensure your own safety.
- **Core to Core.** These boxes point you to content in other modules that might be helpful in understanding the topic being discussed and reference content that you may find on both the Core 1 and Core 2 exams.

- **End-of-Module Material.** Each module closes with the following features, which reinforce the material covered in the module and provide real-world, hands-on testing:
  - **Module Summary:** This bulleted list of concise statements summarizes all major points of the module.
  - **Key Terms:** The content of each module is further reinforced by an end-of-module key term list. The definitions of all terms are included with this text in a full-length glossary.
  - **Thinking Critically Questions:** You can test your understanding of each module with a comprehensive set of "Thinking Critically" questions to help you synthesize and apply what you've learned in scenarios that test your skills at the same depth as the A+ exams.
  - **Hands-On Projects:** These sections give you practice using the skills you have just studied so that you can learn by doing and know you have mastered a skill.
  - **Real Problems, Real Solutions:** Each comprehensive problem allows you to find out if you can apply what you've learned in the module to a real-life situation.
- **Student Companion Site.** Additional content included on the companion website includes information on electricity and multimeters as well as FAT details. Other helpful online references include Frequently Asked Questions, sample reports, a "Computer Inventory and Maintenance" form, and troubleshooting flowcharts.

What's New in the Eleventh Edition

Here's a summary of what's new in the Eleventh Edition:

- Content maps to all of the latest CompTIA's A+ Core 1 and Core 2 exams.
- There is a clean split between Core 1 and Core 2 modules. No module contains overlapping content.
- The modules focus on Windows 10 with some content about Windows 11, which is the same approach taken on the A+ Core 2 exam.
- New content is added (all new content was also new to the A+ Core 1 and Core 2 exams).
  - Windows 11 is added. Operating systems covered now include Windows 10 and Windows 11. Windows 8 and Windows 7 are no longer covered. New content on Linux, macOS, and mobile operating systems (Android, iOS, and iPadOS) is added.
  - Enhanced content on DNS, security, backups, call tracking, and troubleshooting is included in various modules.
  - Because we no longer have modules that contain a mix of Core 1 and Core 2 content, the new Core 2 module "Network Security and Troubleshooting" has been added, with enhanced coverage of these topics. Before studying this module, it is suggested you complete the Core 1 modules "Networking Fundamentals" and "Network Infrastructure and Cloud Computing."
  - To address new content on mobile devices, we have two modules on this topic: the Core 1 module "Supporting Mobile Devices" and the Core 2 module "Mobile Device Security."
  - New content on the macOS has been added, and this topic now has its own Core 2 module, "Supporting macOS."
  - New content on Linux and understanding and writing scripts is covered in the module "Linux and Scripting."
  - Hands-On Projects in several modules use virtual machines so that you get plenty of practice using this essential cloud technology.

Features of the New Edition

Module Objectives appear at the beginning of each module, so you know exactly what topics and skills are covered.

A+ **Exam Tips** include key points pertinent to the A+ exams. The icons identify the sections that cover information you will need to know for the A+ certification exams.

Taking a Computer Apart and Putting It Back Together

Module Objectives

1 Disassemble and reassemble a desktop computer safely, and identify external ports and major components inside a desktop. Describe how they connect and are compatible. Identify various tools you will need as a computer hardware technician.

2 Disassemble and reassemble a laptop computer safely, and

Core 1 Certification Objectives

1.1 Given a scenario, install and configure laptop hardware and components.

1.3 Given a scenario, set up and configure accessories and ports of mobile devices.

2.8 Given a scenario, use networking tools.

3.1 Explain basic cable types and their connectors, features, and purposes.

Exam Tip ✔

As you work your way through the modules and the appendix, notice the A+ Core 1 and Core 2 exam objective numbers that follow certain headings. This information identifies how the content maps to the exam objectives. In the text, A+ Core 1 objective numbers are tagged in teal, and A+ Core 2 objective numbers are tagged in orange. After studying each module or appendix, take a look at the grid at the beginning of this text, and make sure you understand each objective listed in the grid for the module or appendix just completed.

Caution ❗

When you power down a computer and even turn off the power switch on the rear of the computer case, residual power is still on. Some motherboards have a small light inside the case to remind you of this fact and to warn you that power is still getting to the system. Therefore, be sure to always unplug the power cord before opening a case.

Cautions identify critical safety information.

Visual full-color graphics, photos, and screenshots accurately depict computer hardware and software components.

Figure 1-21   The dual-voltage selector switch sets the input voltage to the power supply

Dual-voltage selector switch

Four screws hold the power supply in the case

Note 2

If you ever need to change the dual-voltage selector switch, be sure you first turn off the computer and unplug the power supply.

Form Factors Used by Desktop Cases, Power Supplies, and Motherboards

Applying Concepts

Manage Cellular Data and Roaming

Est. Time: 15 minutes
Core 1 Objective: 1.4

Looking back at Figure 9-14, you can see that a smartphone can use cellular data or Wi-Fi to access the Internet. In certain situations, you might want to disable cellular data or disable cellular roaming. The advantage of disabling cellular data and using Wi-Fi for data transmissions is that Wi-Fi transmissions are not charged against your cellular data subscription plan. Also, Wi-Fi is generally faster than most cellular connections. (When you disable cellular data, you can still send SMS texts because these texts use the carrier's network and not the Internet.) Disabling roaming can prevent roaming charges on your bill incurred from using other carriers' cellular networks when you travel outside your home territory.

To disable roaming on an Android device, go to the **Network & internet** menu in the Settings app, tap **Mobile network**, and then disable **Roaming**. On an iOS device, open the Settings app, tap **Cellular** (see Figure 9-16A), and turn off **Cellular Data**. Next, tap **Cellular Data Options**, and then turn off roaming. On the Cellular Data Options screen, you can also turn on Low Data Mode to conserve cellular data usage. See Figure 9-16B.

Figure 9-16   Control (A) data usages and (B) data roaming in iOS
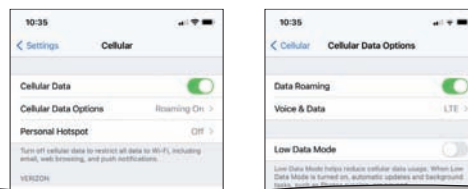
If you have roaming enabled, especially for a CDMA device, you'll want to keep the **Preferred Roaming List (PRL)** updated. The PRL is a database file that lists the preferred service providers or radio frequencies your carrier wants the device to use when outside your home network. To update the PRL, follow instructions from your carrier. For example, for

9

Notes indicate additional content that might be of student interest or information about how best to study.

Applying Concepts sections provide practical advice or pointers by illustrating basic principles, identifying common problems, providing steps to practice skills, and encouraging solutions.

Module Summary bulleted lists of concise statements summarize all major points of the module, organized by primary headings.

Module Summary

9

Mobile Devices, Operating Systems, Connections, and Accessories

- An IT support technician might be called on to service mobile devices such as smartphones and tablets, and, therefore, needs to know the basics of using and supporting Android, iOS, and iPadOS mobile operating systems.
- A mobile device might have several antennas for wireless connections—primarily Wi-Fi, GPS, Bluetooth, NFC, and cellular. The device uses a Wi-Fi or cellular antenna to connect to a LAN (local area network), a WAN (wide area network), or to create its own hotspot, and it uses Bluetooth or NFC to connect to a PAN (personal area network). A wired connection might use a microUSB, miniUSB, USB-C, or proprietary port, such as the Lightning port by Apple, for syncing with a computer or tethering to provide the computer with

Key Terms

For explanations of key terms, see the Glossary for this text.

2G	CDMA (Code Division	IMSI (International	near-field
3G	Multiple Access)	Mobile Subscriber	communication
4G	cellular data	Identity)	(NFC)
4G LTE	commercial mail app	iOS	notifications
5G	dock	iPad	off-boarding
ActiveSync	favorites tray	iPadOS	on-boarding
agent	Google account	iPhone	paired
AirDrop	Google Play	Lightning port	Preferred Roaming
Android	GPS (Global Positioning	MDM policies	List (PRL)
app drawer	System)	Microsoft 365	RFID (radio-frequency

Thinking Critically

These questions are designed to prepare you for the critical thinking required for the A+ exams and may use information from other modules and the web.

1. Which of these network connections would allow your smartphone to sync your photos to your online account? (Choose all that apply.)

   a. Wi-Fi
   b. Bluetooth
   c. GPS
   d. Cellular

2. While visiting a coffee shop, you see a poster advertising a concert for a music group you'd love to see. You notice there's an NFC tag at the bottom with additional information about the concert. Which of the following devices would likely be able to read the NFC tag?

   a. GPS
   b. Smartphone
   c. eReader
   d. Laptop

3. You work for a company that provides the same smartphone model for dozens of its employees. While

Key Terms are defined as they are introduced and listed at the end of each module. Definitions can be found in the Glossary.

Thinking Critically sections require you to analyze and apply what you've learned.

Hands-On Project 1-4

Closing the Case

Est. Time: 15 minutes
Core 1 Objective: 3.4

The case cover to your desktop computer is off from doing the previous exercises. Before you close your case, it's always a good idea to quickly clean it first. Using a can of compressed air, blow the dust away from fans and other components inside the case. Be careful not to touch components unless you are properly grounded. When you're done, close the case cover.

Real Problems, Real Solutions

Real Problem 1-1

Planning Your Computer Repair Toolkit

Est. Time: 30 minutes
Core 1 Objectives: 2.8, 3.4

Do research online to find the following tools for sale: ESD strap, set of flathead and Phillips-head screwdrivers, can of compressed air, monitor-cleaning wipes, multimeter, power supply tester, cable ties, flashlight, loopback plug to test an Ethernet port, POST diagnostic card, and toolbox.

(continues)

Real Problems, Real Solutions allow you to apply what you've learned in the module to a real-life situation.

Hands-On Projects provide practical exercises at the end of each module so that you can practice the skills as they are learned.

What's New with CompTIA® A+ Certification

The CompTIA A+ certification includes two exams, and you must pass both to become CompTIA A+ certified. The two exams are Core 1 (220-1101) and Core 2 (220-1102).

Here is a breakdown of the domain content covered on the two A+ exams.

CompTIA A+ 220-1101 Exam	
Domain	Percentage of Examination
1.0 Mobile Devices	15%
2.0 Networking	20%
3.0 Hardware	25%
4.0 Virtualization and Cloud Computing	11%
5.0 Hardware and Network Troubleshooting	29%
Total	**100%**

CompTIA A+ 220-1102 Exam	
Domain	Percentage of Examination
1.0 Operating Systems	31%
2.0 Security	25%
3.0 Software Troubleshooting	22%
4.0 Operational Procedures	22%
Total	**100%**

Instructor's Materials

Please visit *cengage.com* and log in to access instructor-specific resources, which include the Instructor's Manual, Solutions Manual, test-creation tools, PowerPoint Presentation, and Syllabus.

Instructor's Manual: The Instructor's Manual that accompanies this textbook includes additional instructional material to assist in class preparation, including suggestions for classroom activities, discussion topics, and additional projects.

Solutions: Answers or solution guidance to the end-of-module material are provided. These include the answers to the Thinking Critically questions and solution guidance to the Hands-On Projects and Real Problems, Real Solutions exercises, as well as Lab Manual Solutions.

Cengage Learning Testing Powered by Cognero: This flexible, online system allows you to do the following:

- Author, edit, and manage test bank content from multiple Cengage Learning solutions.
- Create multiple test versions in an instant.
- Deliver tests from your LMS, your classroom, or wherever you want.

PowerPoint Presentations: This text comes with Microsoft PowerPoint slides for each module. These are included as a teaching aid for classroom presentation, to make available to students on the network for module review, or to be printed for classroom distribution. Instructors, please feel free to add your own slides for additional topics you introduce to the class.

Total Solutions for CompTIA A+

MindTap for A+ Guide to IT Technical Support, Eleventh Edition

MindTap is an online learning solution designed to help students master the skills they need in today's workforce. Research shows employers need critical thinkers, troubleshooters, and creative problem-solvers to stay relevant in our fast-paced, technology-driven world. MindTap helps you achieve this with assignments and activities that provide hands-on practice, real-life relevance, mastery of difficult concepts, and certification test prep. Students are guided through assignments that progress from basic knowledge and understanding before moving on to more challenging problems. MindTap features include the following:

- Live Virtual Machine labs allow you to practice, explore, and try different solutions in a safe sandbox environment.
- The Adaptive Test Prep (ATP) app is designed to help you quickly review and assess your understanding of key IT concepts. Test yourself multiple times to track your progress and improvement by filtering results by correct answer, by all questions answered, or by only incorrect answers to show where additional study help is needed.
- IT for Life assignments encourage you to stay current with what's happening in the IT field.
- Pre- and Post-Quizzes assess your understanding of key concepts at the beginning and end of the course.
- All new Reflection activities encourage classroom and online discussion of key issues covered in the modules.

MindTap is designed around learning objectives and provides the analytics and reporting so the instructor can easily see where the class stands in terms of progress, engagement, and completion rates. Use the content and learning path as is, or pick and choose how our materials will wrap around the course as it is taught. The instructor controls what the students see and when they see it. Learn more at *cengage.com/mindtap*.

- Instant Access Code: ISBN: 9780357674185
- Printed Access Code: ISBN: 9780357674185

Lab Manual for A+ Guide to IT Technical Support, Eleventh Edition

The Lab Manual, both in print and as part of your MindTap course, contains over 110 labs to provide students with additional hands-on experience and to help prepare for the A+ exam. The Lab Manual includes lab activities, objectives, materials lists, step-by-step procedures, illustrations, and review questions.

- Lab Manual ISBN: 9780357674567

Acknowledgments

Thank you to the wonderful people at Cengage who continue to give their best and go the extra mile to make the books what they are: Mark Santee, Natalie Onderdonk, and Brooke Greenhouse. We're grateful for all you've done. Thank you, Mary Pat Shaffer, our Developmental Editor extraordinaire, for upholding us with your unwavering, calm demeanor in the face of impossible schedules and inboxes, and to Elizabeth Kelly, our excellent copyeditor/proofreader. Thank you, Danielle Shaw, for your careful attention to the technical accuracy of the book.

Thank you to all the people who took the time to voluntarily send encouragement and suggestions for improvements to the previous editions. Your input and help are very much appreciated. The reviewers of this edition provided invaluable insights and showed a genuine interest in the book's success. Thank you to:

Luis Alfonso Lopez Lerma – Southwest University at El Paso

Kimberly Perez – Tidewater Community College

Gregg Tennefoss – Tidewater Community College

To the instructors and learners who use this book, we invite and encourage you to send suggestions or corrections for future editions. Please write to the author team at *jean.andrews@cengage.com*. We never ignore a good idea! And to instructors, if you have ideas for how to make a class in A+ Preparation a success, please share your ideas with other instructors!

Thank you to our families and friends who have supported and encouraged us through the writing process.

This book is dedicated to the covenant of God with man on earth.

Jean Andrews, Ph.D.
Joy Dark Shelton
Nicholas Pierce

About the Authors

Jean Andrews has more than 30 years of experience in the computer industry, including more than 13 years in the college classroom. She has worked in a variety of businesses and corporations designing, writing, and supporting application software; managing a help desk for computer support technicians; and troubleshooting wide area networks. Jean has written numerous books on software, hardware, and the Internet, including the best-selling *CompTIA A+ Core 1 Exam Guide to Computing Infrastructure, Tenth Edition*, and *CompTIA A+ Core 2 Exam Guide to Operating Systems and Security, Tenth Edition*. She lives in northern Georgia.

Joy Dark Shelton has worked in the IT field as a help-desk technician providing first-level support for a company with presence in 29 states, a second-tier technician in healthcare IT, and an operations specialist designing support protocols and structures. As a teacher, Joy has taught online courses in IT and has taught English as a Second Language in the United States and South America. She has helped write several technical textbooks with Jean Andrews. She also creates many photographs used in educational content. Joy and her husband, Jason, live in northwest Georgia with their two daughters and Brittany dog.

Nicholas Pierce is an information systems and cybersecurity instructor with a background in radio frequency and network troubleshooting. Nicholas delivers courses to high schools, community colleges, and universities, as well as in the private sector as a contractor with the Department of Defense. Nicholas lives in Virginia Beach, Virginia.

Read This Before You Begin

The following hardware, software, and other equipment are needed to do the Hands-On Projects in each module:

- You need a working desktop computer and laptop that can be taken apart and reassembled. You also need a working computer on which you can install an operating system. These computers can be the same or different computers.
- Troubleshooting skills can better be practiced with an assortment of nonworking expansion cards that can be used to simulate problems.
- Windows 10 Pro is needed for most modules. In addition, Windows 11 is needed for the module "Installing Windows," and macOS is used in the module "Supporting macOS."
- Internet access is needed for most modules.
- Equipment required to work on hardware includes an electrostatic discharge strap and flathead and Phillips-head screwdrivers. In addition, a power supply tester, cable tester, and can of compressed air are useful. Network wiring tools needed for the module "Network Infrastructure and Cloud Computing" include a wire cutter, wire stripper, and crimper.
- An iOS or Android smartphone or tablet is needed for the modules "Supporting Mobile Devices" and "Mobile Device Security."
- A small-office-home-office (SOHO) router that includes a wireless access point is needed for the modules "Networking Fundamentals" and "Network Security and Troubleshooting."

Caution ⚠️

Before undertaking any of the lab exercises, starting with the module "Taking a Computer Apart and Putting It Back Together," please review the safety guidelines in the appendix "Safety Procedures and Environmental Concerns."

CompTIA.

Your Next Move Starts Here!

Get CompTIA certified to help achieve your career goals and gain a powerful, vendor-neutral credential that is trusted by employers.

Why get CompTIA certified?

Increase your confidence
91% of certification earners show increased confidence.*

Earn more money
77% of IT pros got a raise within six months of earning their certification.*

Stand out to employers
64% of IT decision makers say certified employers add additional value.**

Join a global community
92% of IT professionals hold at least one certification.**

Get ready for exam day.

• **Download the exam objectives:** Visit CompTIA.org to find the exam objectives for your IT certification and print them out. This is your roadmap!

• **Create your study plan:** Decide how many hours each week you are going to dedicate to studying, choose your preferred study tools and get to work. Studying is a unique experience. Download a study plan worksheet on CompTIA.org.

• **Get certified:** If you haven't already, use the coupon on this page when you purchase your exam voucher and schedule your exam. CompTIA offers flexible testing options to fit your busy life.

Choose your testing option.

Online testing
Earn a CompTIA certification online, from your home – or any quiet, distraction-free, secure location – at a time that's convenient for you.

In-person testing
Test at any of the Pearson VUE test centers around the world, where you can use their equipment under the supervision of a proctor.

To purchase your exam voucher and learn how to prepare for exam day, visit CompTIA.org.

*Pearson VUE 2021 Value of IT Certifications
**2021 Global Knowledge IT Skills and Salary Report

Part

1

CompTIA A+ **Core 1 (220-1101)**