

TestOut PC Pro – English 6.0.x

CompTIA A+ Guide
to IT Technical
Support
(Comprehensive)

TestOut PC Pro v6.0

Objective Mapping: CompTIA 220-1001 Objectives to LabSim Section

ISBN: 978-
0357108291

ISBN: 978-1-935080-
42-8

Author: Jean
Andrews, Joy Dark,
Jill West

Author: TestOut

#	Domain	Chapter	Section
1.0	Mobile Devices	Chapter	Section
1.1	Given a scenario, install and configure laptop hardware and components.	1, 2, 3, 4, 5, 6	
1.1	Hardware/device replacement	1	
1.1	o Keyboard	5	
1.1	o Hard drive - SSD vs. hybrid vs. magnetic disk	5	
1.1	o Hard drive - 1.8in vs. 2.5in	5	
1.1	o Memory	3	
1.1	o Smart card reader	5	
1.1	o Optical drive	5	
1.1	o Wireless card/Bluetooth module	6	
1.1	o Cellular card	6	5.1, 9.2
1.1	o Video card	6	
1.1	o Mini PCIe	6	
1.1	o Screen	6	
1.1	o DC jack	4	
1.1	o Battery	1	
1.1	o Touchpad	6	
1.1	o Plastics/frames	1	
1.1	o Speaker	6	
1.1	o System board	2	
1.1	o CPU	3	
1.2	Given a scenario, install components within the display of a laptop.	6	
1.2	Types	6	
1.2	o LCD	6	
1.2	o OLED	6	1.2, 4.1, 7.1, 9.2, 9.4, 9.5
1.2	WiFi antenna connector/placement	6	
1.2	Webcam	6	
1.2	Microphone	6	
1.2	Inverter	6	
1.2	Digitizer/touchscreen	6	
1.3	Given a scenario, use appropriate laptop features.	1	
1.3	Special function keys	1	
1.3	o Dual displays	1	
1.3	o Wireless (on/off)	1	
1.3	o Cellular (on/off)	1	
1.3	o Volume settings	1	
1.3	o Screen brightness	1	
1.3	o Bluetooth (on/off)	1	
1.3	o Keyboard backlight	1	9.1
1.3	o Touchpad (on/off)	1	
1.3	o Screen orientation	1	
1.3	o Media options (fast forward/rewind)	1	
1.3	o GPS (on/off)	1	
1.3	o Airplane mode	1	
1.3	Docking station	1	

1.3	Port replicator	1	
1.3	Physical laptop lock and cable lock	1	
1.3	Rotating/removable screens	1	
1.4	Compare and contrast characteristics of various types of other mobile devices.	9	
1.4	Tablets	9	
1.4	Smartphones	9	
1.4	Wearable technology devices	9	
1.4	o Smart watches	9	9.5
1.4	o Fitness monitors	9	
1.4	o VR/AR headsets	9	
1.4	E-readers	9	
1.4	GPS	9	
1.5	Given a scenario, connect and configure accessories and ports of other mobile devices.	9	
1.5	Connection types	9	
1.5	o Wired - Micro-USB/Mini-USB/USB-C	9	
1.5	o Wired - Lightning	9	
1.5	o Wired - Tethering	9	
1.5	o Wired - Proprietary vendor-specific ports (communication/power)	9	
1.5	o Wireless - NFC	9	
1.5	o Wireless - Bluetooth	9	
1.5	o Wireless - IR	9	
1.5	o Wireless - Hotspot	9	6.10, 7.2, 7.3, 9.5, 9.6
1.5	Accessories	9	
1.5	o Headsets	9	
1.5	o Speakers	9	
1.5	o Game pads	9	
1.5	o Extra battery packs/battery chargers	9	
1.5	o Protective covers/waterproofing	9	
1.5	o Credit card readers	9	
1.5	o Memory/MicroSD	9	
1.6	Given a scenario, configure basic mobile device network connectivity and application sup	9	
1.6	Wireless/cellular data network (enable/disable)	9	
1.6	o Hotspot	9	
1.6	o Tethering	9	
1.6	o Airplane mode	9	
1.6	Bluetooth	9	
1.6	o Enable Bluetooth	9	
1.6	o Enable pairing	9	
1.6	o Find a device for pairing	9	
1.6	o Enter the appropriate pin code	9	
1.6	o Test connectivity	9	
1.6	Corporate and ISP email configuration	9	
1.6	o POP3	9	7.2, 9.5, 9.6
1.6	o IMAP	9	
1.6	o Port and SSL settings	9	
1.6	o S/MIME	9	
1.6	Integrated commercial provider email configuration	9	
1.6	o iCloud	9	
1.6	o Google/Inbox	9	
1.6	o Exchange Online	9	
1.6	o Yahoo	9	
1.6	PRI updates/PRL updates/baseband updates	9	
1.6	Radio firmware	9	
1.6	IMEI vs. IMSI	9	
1.6	VPN	9	
1.7	Given a scenario, use methods to perform mobile device synchronization.	9	
1.7	Synchronization methods	9	
1.7	o Synchronize to the cloud	9	
1.7	o Synchronize to the desktop	9	
1.7	o Synchronize to the automobile	9	

1.7	Types of data to synchronize	9	
1.7	o Contacts	9	
1.7	o Applications	9	
1.7	o Email	9	
1.7	o Pictures	9	
1.7	o Music	9	
1.7	o Videos	9	9.6
1.7	o Calendar	9	
1.7	o Bookmarks	9	
1.7	o Documents	9	
1.7	o Location data	9	
1.7	o Social media data	9	
1.7	o E-books	9	
1.7	o Passwords	9	
1.7	Mutual authentication for multiple services (SSO)	9	
1.7	Software requirements to install the application on the PC	9	
1.7	Connection types to enable synchronization	9	
2.0	Networking		
2.1	Compare and contrast TCP and UDP ports, protocols, and their purposes.	8	
2.1	Ports and protocols	8	
2.1	o 21 – FTP	8	
2.1	o 22 – SSH	8	
2.1	o 23 – Telnet	8	
2.1	o 25 – SMTP	8	
2.1	o 53 – DNS	8	
2.1	o 80 – HTTP	8	
2.1	o 110 – POP3	8	
2.1	o 143 – IMAP	8	
2.1	o 443 – HTTPS	8	6.5
2.1	o 3389 – RDP	8	
2.1	o 137-139 – NetBIOS/NetBT	8	
2.1	o 445 – SMB/CIFS	8	
2.1	o 427 – SLP	8	
2.1	o 548 – AFP	8	
2.1	o 67/68 – DHCP	8	
2.1	o 389 – LDAP	8	
2.1	o 161/162 – SNMP	8	
2.1	TCP vs. UDP	8	
2.2	Compare and contrast common networking hardware devices.	7, 8, 10	
2.2	Routers	7	
2.2	Switches	8	
2.2	o Managed	8	
2.2	o Unmanaged	8	
2.2	Access points	8	
2.2	Cloud-based network controller	10	
2.2	Firewall	8	
2.2	Network interface card	7	6.2, 6.4, 6.8, 10.5
2.2	Repeater	8	
2.2	Hub	8	
2.2	Cable/DSL modem	7	
2.2	Bridge	8	
2.2	Patch panel	8	
2.2	Power over Ethernet (PoE)	8	
2.2	o Injectors	8	
2.2	o Switch	8	
2.2	Ethernet over Power	8	
2.3	Given a scenario, install and configure a basic wired/wireless SOHO network.	7, 9	
2.3	Router/switch functionality	7	
2.3	Access point settings	7	
2.3	IP addressing	7	

2.3	NIC configuration	7	
2.3	o Wired	7	
2.3	o Wireless	7	
2.3	End-user device configuration	7	
2.3	IoT device configuration	9	
2.3	o Thermostat	9	
2.3	o Light switches	9	
2.3	o Security cameras	9	
2.3	o Door locks	9	
2.3	o Voice-enabled, smart speaker/digital assistant	9	6.8, 7.1, 7.3, 7.4, 13.9
2.3	Cable/DSL modem configuration	7	
2.3	Firewall settings	7	
2.3	o DMZ	7	
2.3	o Port forwarding	7	
2.3	o NAT	7	
2.3	o UPnP	7	
2.3	o Whitelist/blacklist	7	
2.3	o MAC filtering	7	
2.3	QoS	7	
2.3	Wireless settings	7	
2.3	o Encryption	7	
2.3	o Channels	7	
2.3	o QoS	7	
2.4	Compare and contrast wireless networking protocols.	7, 9	
2.4	802.11a	7	
2.4	802.11b	7	
2.4	802.11g	7	
2.4	802.11n	7	
2.4	802.11ac	7	
2.4	Frequencies	7	
2.4	o 2.4Ghz	7	
2.4	o 5Ghz	7	
2.4	Channels	7	7.1, 7.2, 7.3, 7.4, 9.6,
2.4	o 1–11	7	13.7
2.4	Bluetooth	9	
2.4	NFC	9	
2.4	RFID	9	
2.4	Zigbee	9	
2.4	Z-Wave	9	
2.4	3G	7	
2.4	4G	7	
2.4	5G	7	
2.4	LTE	7	
2.5	Summarize the properties and purposes of services provided by networked hosts.	8	
2.5	Server roles	8	
2.5	o Web server	8	
2.5	o File server	8	
2.5	o Print server	8	
2.5	o DHCP server	8	
2.5	o DNS server	8	
2.5	o Proxy server	8	4.5, 6.2, 7.1, 13.6,
2.5	o Mail server	8	13.10, 13.11
2.5	o Authentication server	8	
2.5	o syslog	8	
2.5	Internet appliance	8	
2.5	o UTM	8	
2.5	o IDS	8	
2.5	o IPS	8	

2.5	○ End-point management server	8	
2.5	Legacy/embedded systems	8	
2.6	Explain common network configuration concepts.	7, 8	
2.6	IP addressing	8	
2.6	○ Static	8	
2.6	○ Dynamic	8	
2.6	○ APIPA	8	
2.6	○ Link local	8	
2.6	DNS	8	6.6, 6.7, 7.3, 9.6, 10.5, 13.12
2.6	DHCP	8	
2.6	○ Reservations	7	
2.6	IPv4 vs. IPv6	8	
2.6	Subnet mask	8	
2.6	Gateway	8	
2.6	VPN	7	
2.6	VLAN	8	
2.6	NAT	8	
2.7	Compare and contrast Internet connection types, network types, and their features.	7	
2.7	Internet connection types	7	
2.7	○ Cable	7	
2.7	○ DSL	7	
2.7	○ Dial-up	7	
2.7	○ Fiber	7	
2.7	○ Satellite	7	
2.7	○ ISDN	7	
2.7	○ Cellular - Tethering	7	6.1, 6.8
2.7	○ Cellular - Mobile hotspot	7	
2.7	○ Line-of-sight wireless Internet service	7	
2.7	Network types	7	
2.7	○ LAN	7	
2.7	○ WAN	7	
2.7	○ PAN	7	
2.7	○ MAN	7	
2.7	○ WMN	7	
2.8	Given a scenario, use appropriate networking tools.	8	
2.8	Crimper	8	6.10, 7.5
2.8	Cable stripper	8	
2.8	Multimeter	8	
2.8	Tone generator and probe	8	
2.8	Cable tester	8	
2.8	Loopback plug	8	
2.8	Punchdown tool	8	
2.8	WiFi analyzer	8	
3.0	Hardware		
3.1	Explain basic cable types, features, and their purposes.	5, 6, 8, 9	
3.1	Network cables	8	
3.1	○ Ethernet - Cat 5	8	
3.1	○ Ethernet - Cat 5e	8	
3.1	○ Ethernet - Cat 6	8	
3.1	○ Ethernet - Plenum	8	
3.1	○ Ethernet - Shielded twisted pair	8	
3.1	○ Ethernet - Unshielded twisted pair	8	
3.1	○ Ethernet - 568A/B	8	
3.1	○ Fiber	8	
3.1	○ Coaxial	8	
3.1	○ Speed and transmission limitations	8	
3.1	Video cables	6	
3.1	○ VGA	6	
3.1	○ HDMI	6	
3.1	○ Mini-HDMI	6	

3.1	○ DisplayPort	6	1.2, 3.12, 4.2
3.1	○ DVI	6	5.1, 5.2
3.1	○ DVI-DDVI-I	6	6.3, 6.4
3.1	Multipurpose cables	6, 9	9.6
3.1	○ Lightning	9	
3.1	○ Thunderbolt	6	
3.1	○ USB	6	
3.1	○ USB-C	6	
3.1	○ USB 2.0	6	
3.1	○ USB 3.0	6	
3.1	Peripheral cables	6	
3.1	○ Serial	6	
3.1	Hard drive cables	5	
3.1	○ SATA	5	
3.1	○ IDE	5	
3.1	○ SCSI	5	
3.1	Adapters	6	
3.1	○ DVI to HDMI	6	
3.1	○ USB to Ethernet	6	
3.1	○ DVI to VGA	6	
3.2	Identify common connector types.	2, 5, 6, 7	
3.2	RJ-11	7	
3.2	RJ-45	7	
3.2	RS-232	6	
3.2	BNC	6	
3.2	RG-59	6	
3.2	RG-6	6	
3.2	USB	6	1.2, 3.2, 3.12, 4.2, 5.1, 5.2, 6.3, 9.6
3.2	Micro-USB	6	
3.2	Mini-USB	6	
3.2	USB-C	6	
3.2	DB-9	6	
3.2	Lightning	6	
3.2	SCSI	5	
3.2	eSATA	5	
3.2	Molex	2	
3.3	Given a scenario, install RAM types.	3	
3.3	RAM types	3	
3.3	○ SODIMM	3	
3.3	○ DDR2	3	
3.3	○ DDR3	3	
3.3	○ DDR4	3	
3.3	Single channel	3	3.7, 3.8
3.3	Dual channel	3	
3.3	Triple channel	3	
3.3	Error correcting	3	
3.3	Parity vs. non-parity	3	
3.4	Given a scenario, select, install and configure storage devices.	5	
3.4	Optical drives	5	
3.4	○ CD-ROM/CD-RW	5	
3.4	○ DVD-ROM/DVD-RW/DVD-RW DL	5	
3.4	○ Blu-ray	5	
3.4	○ BD-R	5	
3.4	○ BD-RE	5	
3.4	Solid-state drives	5	
3.4	○ M2 drives	5	
3.4	○ NVME	5	
3.4	○ SATA 2.5	5	
3.4	Magnetic hard drives	5	
3.4	○ 5,400rpm	5	

3.4	o 7,200rpm	5	3.3, 4.5, 5.1, 5.2, 5.3, 5.4, 5.9, 9.1, 9.2
3.4	o 10,000rpm	5	
3.4	o 15,000rpm	5	
3.4	o Sizes - 2.5	5	
3.4	o Sizes - 3.5	5	
3.4	Hybrid drives	5	
3.4	Hybrid drives	5	
3.4	Flash	5	
3.4	o SD card	5	
3.4	o CompactFlash	5	
3.4	o Micro-SD card	5	
3.4	o Mini-SD card	5	
3.4	o xD	5	
3.4	Configurations	5	
3.4	o RAID 0, 1, 5, 10	5	
3.4	o Hot swappable	5	
3.5	Given a scenario, install and configure motherboards, CPUs, and add-on cards.	1, 2, 3	3.1, 3.3, 3.5, 3.10, 3.11, 3.12, 3.13, 3.14, 4.2, 5.1, 5.2, 6.2, 9.2, 13.5
3.5	Motherboard form factor	2	
3.5	o ATX	2	
3.5	o mATX	2	
3.5	o ITX	2	
3.5	o mITX	2	
3.5	Motherboard connectors types	1, 2	
3.5	o PCI	2	
3.5	o PCIe	2	
3.5	o Riser card	2	
3.5	o Socket types	2	
3.5	o SATA	2	
3.5	o IDE	2	
3.5	o Front panel connector	1	
3.5	o Internal USB connector BIOS/UEFI settings	2	
3.5	o Boot options	2	
3.5	o Firmware updates	2	
3.5	o Security settings	2	
3.5	o Interface configurations	2	
3.5	o Security - Passwords	2	
3.5	o Security - Drive encryption - TPM	2	
3.5	o Security - Drive encryption - LoJack	2	
3.5	o Security - Drive encryption - Secure boot CMOS battery	2	
3.5	CPU features	3	
3.5	o Single-core	3	
3.5	o Multicore	3	
3.5	o Virtual technology	3	
3.5	o Hyperthreading	3	
3.5	o Speeds	3	
3.5	o Overclocking	3	
3.5	o Integrated GPU	3	
3.5	Compatibility	3	
3.5	o AMD	3	
3.5	o Intel	3	
3.5	Cooling mechanism	3	
3.5	o Fans	3	
3.5	o Heat sink	3	
3.5	o Liquid	3	
3.5	o Thermal paste	3	
3.5	Expansion cards	3	
3.5	o Video cards - Onboard	3	
3.5	o Video cards - Add-on card	3	
3.5	o Sound cards	3	
3.5	o Network interface card	3	
3.5	o USB expansion card	3	

3.5	o eSATA card	3	
3.6	Explain the purposes and uses of various peripheral types.	5, 6, 10	
3.6	Printer	10	
3.6	ADF/flatbed scanner	10	
3.6	Barcode scanner/QR scanner	6	
3.6	Monitors	6	
3.6	VR headset	6	
3.6	Optical DVD drive	5	
3.6	Mouse	5	
3.6	Keyboard	6	
3.6	Touchpad	6	
3.6	Signature pad	6	1.2, 3.12, 3.13, 4.1,
3.6	Game controllers	6	4.2, 4.4, 5.3, 8.2, 9.5,
3.6	Camera/webcam	6	10.2, 13.7
3.6	Microphone	6	
3.6	Speakers	6	
3.6	Headset	6	
3.6	Projector	6	
3.6	o Lumens/brightness	6	
3.6	External storage drives	5	
3.6	KVM	6	
3.6	Magnetic reader/chip reader	6	
3.6	NFC/tap pay device	6	
3.6	Smart card reader	5	
3.7	Summarize power supply types and features.	4	
3.7	Input 115V vs. 220V	4	
3.7	Output 5.5V vs. 12V	4	
3.7	24-pin motherboard adapter	4	3.2
3.7	Wattage rating	4	
3.7	Number of devices/types of devices to be powered	4	
3.8	Given a scenario, select and configure appropriate components for a custom PC configuration	5, 6, 10	
3.8	Graphic/CAD/CAM design workstation	6	
3.8	o Multicore processor	6	
3.8	o High-end video	6	
3.8	o Maximum RAM	6	
3.8	Audio/video editing workstation	6	
3.8	o Specialized audio and video card	6	
3.8	o Large, fast hard drive	6	
3.8	o Dual monitors	6	
3.8	Virtualization workstation	10	
3.8	o Maximum RAM and CPU cores	10	
3.8	Gaming PC	6	
3.8	o Multicore processor	6	
3.8	o High-end video/specialized GPU	6	
3.8	o High-definition sound card	6	
3.8	o High-end cooling	6	
3.8	Standard thick client	10	
3.8	o Desktop applications	10	
3.8	o Meets recommended requirements for selected OS	10	
3.8	Thin client	10	
3.8	o Basic applications	10	
3.8	o Meets minimum requirements for selected OS	10	
3.8	o Network connectivity	10	
3.8	Network attached storage device	5, 6	
3.8	o Media streaming	6	
3.8	o File sharing	6	
3.8	o Gigabit NIC	6	
3.8	o RAID array	5	
3.9	Given a scenario, install and configure common devices.	6, 7, 9, 10	
3.9	Desktop	7, 10	
3.9	o Thin client	10	

3.9	o Thick client	10	
3.9	o Account setup/settings	7	
3.9	Laptop/common mobile devices	6,9	7.1, 9.2, 9.5, 9.6, 10.1,
3.9	o Touchpad configuration	6	10.2, 11.3
3.9	o Touchscreen configuration	6	
3.9	o Application installations/configurations	9	
3.9	o Synchronization settings	9	
3.9	o Account setup/settings	9	
3.9	o Wireless settings	9	
3.10	Given a scenario, configure SOHO multifunction devices/printers and settings.	10	
3.10	Use appropriate drivers for a given operating system	10	
3.10	o Configuration settings - Duplex	10	
3.10	o Configuration settings - Collate	10	
3.10	o Configuration settings - Orientation	10	
3.10	o Configuration settings - Quality	10	
3.10	Device sharing	10	
3.10	o Wired - USB	10	
3.10	o Wired - Serial	10	
3.10	o Wired - Ethernet	10	8.2, 8.3, 8.4
3.10	o Wireless - Bluetooth	10	
3.10	o Wireless - 802.11(a, b, g, n, ac)	10	
3.10	o Wireless - Infrastructure vs. ad hoc	10	
3.10	o Integrated print server (hardware)	10	
3.10	o Cloud printing/remote printing	10	
3.10	Public/shared devices	10	
3.10	o Sharing local/networked device via operating system settings	10	
3.10	TCP/Bonjour/AirPrint	10	
3.10	o Data privacy - User authentication on the device	10	
3.10	o Data privacy - Hard drive caching	10	
3.11	Given a scenario, install and maintain various print technologies.	10	
3.11	Laser	10	
3.11	o Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separate pads, duplexing assembly	10	
3.11	o Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning	10	
3.11	o Maintenance: Replace toner, apply maintenance kit, calibrate, clean	10	
3.11	Inkjet	10	
3.11	o Ink cartridge, print head, roller, feeder, duplexing assembly, carriage, and belt	10	
3.11	o Calibrate	10	
3.11	o Maintenance: Clean heads, replace cartridges, calibrate, clear jams	10	
3.11	Thermal	10	
3.11	o Feed assembly, heating element	10	8.1, 8.2, 8.5
3.11	o Special thermal paper	10	
3.11	o Maintenance: Replace paper, clean heating element, remove debris	10	
3.11	Impact	10	
3.11	o Print head, ribbon, tractor feed	10	
3.11	o Impact paper	10	
3.11	o Maintenance: Replace ribbon, replace print head, replace paper	10	
3.11	Virtual	10	
3.11	o Print to file	10	
3.11	o Print to PDF	10	
3.11	o Print to XPS	10	
3.11	o Print to image	10	
3.11	3D printers	10	
3.11	o Plastic filament	10	

4 Virtualization and Cloud Computing			
4.1	Compare and contrast cloud computing concepts.	9, 10	
4.1	Common cloud models	10	
4.1	o IaaS	10	
4.1	o SaaS	10	
4.1	o PaaS	10	
4.1	o Public vs. private vs. hybrid vs. community	10	
4.1	Shared resources	10	
4.1	o Internal vs. external	10	
4.1	Rapid elasticity	10	
4.1	On-demand	10	
4.1	Resource pooling	10	10.5
4.1	Measured service	10	
4.1	Metered	10	
4.1	Off-site email applications	10	
4.1	Cloud file storage services	9, 10	
4.1	o Synchronization apps	9	
4.1	Virtual application streaming/cloud-based applications	10	
4.1	o Applications for cell phones/tablets	10	
4.1	o Applications for laptops/desktops	10	
4.1	Virtual desktop	10	
4.1	o Virtual NIC	10	
4.2	Given a scenario, set up and configure client-side virtualization.	10	
4.2	Purpose of virtual machines		10.5
	Resource requirements	10	
	Emulator requirements		
	Security requirements		
	Network requirements		
	Hypervisor		
5 Hardware and Network Troubleshooting			
5.1	Given a scenario, use the best practice methodology to resolve problems.	4	
5.1	Always consider corporate policies, procedures, and impacts before implementing change	4	
5.1	1. Identify the problem	4	
5.1	o Question the user and identify user changes to computer and perform backups before making changes	4	
5.1	o Inquire regarding environmental or infrastructure changes	4	
5.1	o Review system and application logs	4	
5.1	2. Establish a theory of probable cause (question the obvious)	4	
5.1	o If necessary, conduct external or internal research based on symptoms	4	2.6
5.1	3. Test the theory to determine cause	4	
5.1	o Once the theory is confirmed, determine the next steps to resolve problem	4	
5.1	o If theory is not confirmed re-establish new theory or escalate	4	
5.1	4. Establish a plan of action to resolve the problem and implement the solution	4	
5.1	5. Verify full system functionality and, if applicable, implement preventive measures	4	
5.1	6. Document findings, actions, and outcomes	4	
5.2	Given a scenario, troubleshoot problems related to motherboards, RAM, CPUs, and power.	4	
5.2	Common symptoms	4	
5.2	o Unexpected shutdowns	4	
5.2	o System lockups	4	
5.2	o POST code beeps	4	
5.2	o Blank screen on bootup	4	
5.2	o BIOS time and setting resets	4	
5.2	o Attempts to boot to incorrect device	4	
5.2	o Continuous reboots	4	
5.2	o No power	4	3.4, 3.9
5.2	o Overheating	4	
5.2	o Loud noise	4	
5.2	o Intermittent device failure	4	
5.2	o Fans spin – no power to other devices	4	
5.2	o Indicator lights	4	

5.2	o Smoke	4	
5.2	o Burning smell	4	
5.2	o Proprietary crash screens (BSOD/pin wheel)	4	
5.2	o Distended capacitors	4	
5.2	o Log entries and error messages	4	
5.3	Given a scenario, troubleshoot hard drives and RAID arrays.	5	
5.3	Common symptoms	5	
5.3	o Read/write failure	5	
5.3	o Slow performance	5	
5.3	o Loud clicking noise	5	
5.3	o Failure to boot	5	5.1
5.3	o Drive not recognized	5	
5.3	o OS not found	5	
5.3	o RAID not found	5	
5.3	o RAID stops working	5	
5.3	o Proprietary crash screens (BSOD/pin wheel)	5	
5.3	o S.M.A.R.T. errors	5	
5.4	Given a scenario, troubleshoot video, projector, and display issues.	6	
5.4	Common symptoms	6	
5.4	o VGA mode	6	
5.4	o No image on screen	6	
5.4	o Overheat shutdown	6	
5.4	o Dead pixels	6	
5.4	o Artifacts	6	
5.4	o Incorrect color patterns	6	4.4
5.4	o Dim image	6	
5.4	o Flickering image	6	
5.4	o Distorted image	6	
5.4	o Distorted geometry	6	
5.4	o Burn-in	6	
5.4	o Oversized images and icons	6	
5.4	o Multiple failed jobs in logs	6	
5.5	Given a scenario, troubleshoot common mobile device issues while adhering to the appropriate procedures.	1, 4, 6, 9	
5.5	Common symptoms	1, 4, 6, 9	
5.5	o No display	6	
5.5	o Dim display	6	
5.5	o Flickering display	6	
5.5	o Sticking keys	1	
5.5	o Intermittent wireless	9	
5.5	o Battery not charging	4	
5.5	o Ghost cursor/pointer drift	6	
5.5	o No power	4	
5.5	o Num lock indicator lights	6	
5.5	o No wireless connectivity	9	
5.5	o No Bluetooth connectivity	9	
5.5	o Cannot display to external monitor	6	
5.5	o Touchscreen non-responsive	9	9.2, 9.4, 9.8
5.5	o Apps not loading	9	
5.5	o Slow performance	9	
5.5	o Unable to decrypt email	9	
5.5	o Extremely short battery life	9	
5.5	o Overheating	9	
5.5	o Frozen system	9	
5.5	o No sound from speakers	9	
5.5	o GPS not functioning	9	
5.5	o Swollen battery	9	
5.5	Disassembling processes for proper reassembly	1	
5.5	o Document and label cable and screw locations	1	

5.5	○ Organize parts	1	
5.5	○ Refer to manufacturer resources	1	
5.5	○ Use appropriate hand tools	1	
5.6	Given a scenario, troubleshoot printers.	10	
5.6	Common symptoms	10	
5.6	○ Streaks	10	
5.6	○ Faded prints	10	
5.6	○ Ghost images	10	
5.6	○ Toner not fused to the paper	10	
5.6	○ Creased paper	10	
5.6	○ Paper not feeding	10	
5.6	○ Paper jam	10	
5.6	○ No connectivity	10	
5.6	○ Garbled characters on paper	10	8.6
5.6	○ Vertical lines on page	10	
5.6	○ Backed-up print queue	10	
5.6	○ Low memory errors	10	
5.6	○ Access denied	10	
5.6	○ Printer will not print	10	
5.6	○ Color prints in wrong print color	10	
5.6	○ Unable to install printer	10	
5.6	○ Error codes	10	
5.6	○ Printing blank pages	10	
5.6	○ No image on printer display	10	
5.7	Given a scenario, troubleshoot common wired and wireless network problems.	8	
5.7	Common symptoms	8	
5.7	○ Limited connectivity	8	
5.7	○ Unavailable resources - Internet	8	
5.7	○ Unavailable resources - Local resources - Shares	8	
5.7	○ Unavailable resources - Local resources - Printers	8	
5.7	○ Unavailable resources - Local resources - Email	8	
5.7	○ No connectivity	8	
5.7	○ APIPA/link local address	8	
5.7	○ Intermittent connectivity	8	
5.7	○ IP conflict	8	
5.7	○ Slow transfer speeds	8	
5.7	○ Low RF signal	8	6.9, 6.10, 7.5
5.7	○ SSID not found	8	
5.7	○ Unavailable resources - Internet	8	
5.7	○ Unavailable resources - Local resources - Shares	8	
5.7	○ Unavailable resources - Local resources - Printers	8	
5.7	○ Unavailable resources - Local resources - Email	8	
5.7	○ No connectivity	8	
5.7	○ APIPA/link local address	8	
5.7	○ Intermittent connectivity	8	
5.7	○ IP conflict	8	
5.7	○ Slow transfer speeds	8	
5.7	○ Low RF signal	8	
5.7	○ SSID not found	8	
TestOut PC Pro – English 6.0.x		CompTIA A+ Guide to IT Technical Support (Comprehensive)	TestOut PC Pro v6.0
Objective Mapping: CompTIA 220-1002 Objectives to LabSim Section		ISBN: 978- 0357108291	ISBN: 978-1-935080- 42-8

#	Domain	Author: Jean Andrews, Joy Dark, Jill West	Author: TestOut
1.0	Operating Systems	Chapter	Section
1.1	Compare and contrast common operating system types and their purposes.	9, 12, 18	
1.1	32-bit vs. 64-bit	12	
1.1	o RAM limitations	12	
1.1	o Software compatibility	12	
1.1	Workstation operating systems	18	
1.1	o Microsoft Windows	18	
1.1	o Apple Macintosh OS	18	
1.1	o Linux	18	
1.1	Cell phone/tablet operating systems	9	1.3, 1.4, 1.5, 3.5, 9.5, 10.2, 12.1
1.1	o Microsoft Windows	9	
1.1	o Android	9	
1.1	o iOS	9	
1.1	o Chrome OS	9	
1.1	Vendor-specific limitations	18	
1.1	o End-of-life	18	
1.1	o Update limitations	18	
1.1	Compatibility concerns between operating systems	18	
1.2	Compare and contrast features of Microsoft Windows versions.	11	
1.2	Windows 7	11	
1.2	Windows 8	11	
1.2	Windows 8.1	11	
1.2	Windows 10	11	
1.2	Corporate vs. personal needs	11	
1.2	o Domain access	11	10.2, 13.8
1.2	o Bitlocker	11	
1.2	o Media center	11	
1.2	o Branchcache	11	
1.2	o EFS	11	
1.2	Desktop styles/user interface	11	
1.3	Summarize general OS installation considerations and upgrade methods.	12, 13, 15, 18	
1.3	Boot methods	12, 18	
1.3	o USB	12	
1.3	o CD-ROM	12	
1.3	o DVD	12	
1.3	o PXE	12	
1.3	o Solid state/flash drives	18	
1.3	o Netboot	12	
1.3	o External/hot-swappable drive	15	
1.3	o Internal hard drive (partition)	12	
1.3	Type of installations	12, 15	
1.3	o Unattended installation	12	
1.3	o In-place upgrade	12	
1.3	o Clean install	12	
1.3	o Repair installation	15	
1.3	o Multiboot	12	
1.3	o Remote network installation	12	
1.3	o Image deployment	12	
1.3	o Recovery partition	15	
1.3	o Refresh/restore	15	
1.3	Partitioning	13	
1.3	o Dynamic	13	
1.3	o Basic	13	1.5, 5.5, 5.6, 10.2, 10.3, 11.4, 12.10, 12.11, 12.14, 13.2
1.3	o Primary	13	
1.3	o Extended	13	
1.3	o Logical	13	
1.3	o GPT	13	

1.3	File system types/formatting	13, 18	
1.3	o ExFAT	13	
1.3	o FAT32	13	
1.3	o NTFS	13	
1.3	o CDFS	13	
1.3	o NFS	13	
1.3	o ext3, ext4	18	
1.3	o HFS	18	
1.3	o Swap partition	18	
1.3	o Quick format vs. full format	12	
1.3	Load alternate third-party drivers when necessary	12	
1.3	Workgroup vs. Domain setup	11	
1.3	Time/date/region/language settings	12	
1.3	Driver installation, software, and Windows updates	12	
1.3	Factory recovery partition	15	
1.3	Properly formatted boot drive with the correct partitions/format	15	
1.3	Prerequisites/hardware compatibility	12	
1.3	Application compatibility	12	
1.3	OS compatibility/upgrade path	12	
1.4	Given a scenario, use appropriate Microsoft command line tools.	7, 13, 14, 15, 16	
1.4	Navigation	13	
1.4	o dir	13	
1.4	o cd..	13	
1.4	ipconfig	7	
1.4	ping	7	
1.4	tracert	7	
1.4	netstat	7	
1.4	nslookup	7	
1.4	shutdown	13	
1.4	dism	14	
1.4	sfc	14	
1.4	chkdsk	14	5.6, 5.9, 6.9, 10.3, 11.2, 11.4, 12.1, 12.5, 12.15
1.4	diskpart	15	
1.4	taskkill	14	
1.4	gpupdate	16	
1.4	gpreult	16	
1.4	format	13	
1.4	copy	13	
1.4	xcopy	13	
1.4	robocopy	13	
1.4	net use	7	
1.4	net user	7	
1.4	[command name] /?	13	
1.4	Commands available with standard privileges vs. administrative privileges	13	
1.5	Given a scenario, use Microsoft operating system features and tools.	11, 12, 13, 14, 16	
1.5	Administrative	14, 16	
1.5	o Computer Management	14	
1.5	o Device Manager	12	
1.5	o Local Users and Groups	16	
1.5	o Local Security Policy	16	
1.5	o Performance Monitor	14	
1.5	o Services	14	
1.5	o System Configuration	14	
1.5	o Task Scheduler	14	
1.5	o Component Services	14	
1.5	o Data Sources	14	
1.5	o Print Management	14	
1.5	o Windows Memory Diagnostics	14	
1.5	o Windows Firewall	16	
1.5	o Advanced Security	16	
1.5	o Event Viewer	14	

1.5	o User Account Management	16	
1.5	MSConfig	14	
1.5	o General	14	
1.5	o Boot	14	
1.5	o Services	14	
1.5	o Startup	14	
1.5	o Tools	14	
1.5	Task Manager	14	
1.5	o Applications	14	3.9, 4.5, 4.6, 5.6, 5.7,
1.5	o Processes	14	5.8, 5.9, 8.4, 11.4,
1.5	o Performance	14	12.1, 12.3, 12.5, 12.7,
1.5	o Networking	14	12.10, 12.12, 13.7,
1.5	o Users	14	13.10
1.5	Disk Management	13	
1.5	o Drive status	13	
1.5	o Mounting	13	
1.5	o Initializing	13	
1.5	o Extending partitions	13	
1.5	o Splitting partitions	13	
1.5	o Shrink partitions	13	
1.5	o Assigning/changing drive letters	13	
1.5	o Adding drives	13	
1.5	o Adding arrays	13	
1.5	o Storage spaces	13	
1.5	System utilities	11, 12, 13, 14	
1.5	o Regedit	14	
1.5	o Command	13	
1.5	o Services.msc	14	
1.5	o MMC	14	
1.5	o MSTSC	13	
1.5	o Notepad	11	
1.5	o Explorer	11	
1.5	o Msinfo32	11	
1.5	o DxDiag	14	
1.5	o Disk Defragmenter	13	
1.5	o System Restore	14	
1.5	o Windows Update	12	
1.6	Given a scenario, use Microsoft Windows Control Panel utilities.	11, 14, 16	
1.6	Internet Options	16	
1.6	o Connections	16	
1.6	o Security	16	
1.6	o General	16	
1.6	o Privacy	16	
1.6	o Programs	16	
1.6	o Advanced	16	
1.6	Display/Display Settings	14, 16	
1.6	o Resolution	14	
1.6	o Color depth	14	
1.6	o Refresh rate User Accounts	16	
1.6	Folder Options	11	
1.6	o View hidden files	11	
1.6	o Hide extensions	11	
1.6	o General options	11	
1.6	o View options	11	
1.6	System	13, 14	3.13, 4.3, 4.5, 6.6, 8.2,
1.6	o Performance (virtual memory)	14	9.3, 10.2, 11.2, 12.1,
1.6	o Remote settings	13	12.5, 12.6, 12.7,,
1.6	o System protection	13	12.12, 12.13, 13.7,
1.6	Windows Firewall	16	13.8, 13.10

1.6	Power Options	11	
1.6	o Hibernate	11	
1.6	o Power plans	11	
1.6	o Sleep/suspend	11	
1.6	o Standby	11	
1.6	Credential Manager	16	
1.6	Programs and features	12	
1.6	HomeGroup	11	
1.6	Devices and Printers	12	
1.6	Sound	11	
1.6	Troubleshooting	14	
1.6	Network and Sharing Center	11	
1.6	Device Manager	12	
1.6	Bitlocker	16	
1.6	Sync Center	16	
1.7	Summarize application installation and configuration concepts.	12	
1.7	System requirements	12	
1.7	o Drive space	12	
1.7	o RAM	12	
1.7	OS requirements	12	
1.7	o Compatibility	12	
1.7	Methods of installation and deployment	12	3.7, 5.6, 10.2, 10.3, 11.3, 12.1, 13.13
1.7	o Local (CD/USB)	12	
1.7	o Network-based	12	
1.7	Local user permissions	12	
1.7	o Folder/file access for installation	12	
1.7	Security considerations	12	
1.7	o Impact to device	12	
1.7	o Impact to network	12	
1.8	Given a scenario, configure Microsoft Windows networking on a client/desktop.	7, 11, 13, 16	
1.8	HomeGroup vs. Workgroup	11	
1.8	Domain setup	11	
1.8	Network shares/administrative shares/mapping drives	16	
1.8	Printer sharing vs. network printer mapping	16	
1.8	Establish networking connections	7	
1.8	o VPN	7	
1.8	o Dial-ups	7	
1.8	o Wireless	7	
1.8	o Wired	7	
1.8	o WWAN (Cellular)	7	
1.8	Proxy settings	16	
1.8	Remote Desktop Connection	13	
1.8	Remote Assistance	13	
1.8	Home vs. Work vs. Public network settings	11	6.2, 6.4, 6.6, 6.8, 7.1, 8.3, 10.2, 11.4, 12.6, 13.10, 13.11, 13.12
1.8	Firewall settings	16	
1.8	o Exceptions	16	
1.8	o Configuration	16	
1.8	o Enabling/disabling Windows Firewall	16	
1.8	Configuring an alternative IP address in Windows	7	
1.8	o IP addressing	7	
1.8	o Subnet mask	7	
1.8	o DNS	7	
1.8	o Gateway	7	
1.8	Network card properties	7	
1.8	o Half duplex/full duplex/auto	7	
1.8	o Speed	7	
1.8	o Wake-on-LAN	7	
1.8	o QoS	7	
1.8	o BIOS (on-board NIC)	7	

1.9	Given a scenario, use features and tools of the Mac OS and Linux client/desktop operating systems	18	
1.9	Best practices	18	
1.9	o Scheduled backups	18	
1.9	o Scheduled disk maintenance	18	
1.9	o System updates/App Store	18	
1.9	o Patch management	18	
1.9	o Driver/firmware updates	18	
1.9	o Antivirus/Anti-malware updates	18	
1.9	Tools	18	
1.9	o Backup/Time Machine	18	
1.9	o Restore/Snapshot	18	
1.9	o Image recovery	18	
1.9	o Disk maintenance utilities	18	
1.9	o Shell/Terminal	18	
1.9	o Screen sharing	18	
1.9	o Force Quit	18	
1.9	Features	18	
1.9	o Multiple desktops/Mission Control	18	
1.9	o Key Chain	18	
1.9	o Spot Light	18	
1.9	o iCloud	18	
1.9	o Gestures	18	1.4, 1.5, 4.5, 6.9, 11.5,
1.9	o Finder	18	12.1, 12.6, 12.8, 12.10,
1.9	o Remote Disc	18	12.11, 12.12, 13.6
1.9	o Dock	18	
1.9	o Boot Camp	18	
1.9	Basic Linux commands	18	
1.9	o ls	18	
1.9	o grep	18	
1.9	o cd	18	
1.9	o shutdown	18	
1.9	o pwd vs. passwd	18	
1.9	o mv	18	
1.9	o cp	18	
1.9	o rm	18	
1.9	o chmod	18	
1.9	o chown	18	
1.9	o iwconfig/ifconfig	18	
1.9	o ps	18	
1.9	o su/sudo	18	
1.9	o apt-get	18	
1.9	o vi	18	
1.9	o dd	18	
1.9	o kill	18	
2	Security		
2.1	Summarize the importance of physical security measures.	17	
2.1	Mantrap	17	
2.1	Badge reader	17	
2.1	Smart card	17	
2.1	Security guard	17	
2.1	Door lock	17	
2.1	Biometric locks	17	13.3
2.1	Hardware tokens	17	
2.1	Cable locks	17	
2.1	Server locks	17	
2.1	USB locks	17	
2.1	Privacy screen	17	
2.1	Key fobs	17	
2.1	Entry control roster	17	
2.2	Explain logical security concepts.	7, 16, 17	

2.2	Active Directory	16	
2.2	o Login script	16	
2.2	o Domain	16	
2.2	o Group Policy/Updates	16	
2.2	o Organizational Units	16	
2.2	o Home Folder	16	
2.2	o Folder redirection	16	
2.2	Software tokens	17	
2.2	MDM policies	17	
2.2	Port security	17	
2.2	MAC address filtering	7	7.1, 9.7, 12.4, 12.5,
2.2	Certificates	17	13.1, 13.3, 13.6, 13.7,
2.2	Antivirus/Anti-malware	17	13.9, 13.10, 13.12
2.2	Firewalls	16	
2.2	User authentication/strong passwords	16	
2.2	Multifactor authentication	17	
2.2	Directory permissions	16	
2.2	VPN	17	
2.2	DLP	17	
2.2	Access control lists	17	
2.2	Smart card	17	
2.2	Email filtering	17	
2.2	Trusted/untrusted software sources	17	
2.2	Principle of least privilege	16	
2.3	Compare and contrast wireless security protocols and authentication methods.	7, 17	
2.3	Protocols and encryption	7	
2.3	o WEP	7	
2.3	o WPA	7	
2.3	o WPA2	7	
2.3	o TKIP	7	
2.3	o AES	7	7.1, 13.7
2.3	Authentication	17	
2.3	o Single-factor	17	
2.3	o Multifactor	17	
2.3	o RADIUS	17	
2.3	o TACACS	17	
2.4	Given a scenario, detect, remove, and prevent malware using appropriate tools and methods.	17	
2.4	Malware	17	
2.4	o Ransomware	17	
2.4	o Trojan	17	
2.4	o Keylogger	17	
2.4	o Rootkit	17	
2.4	o Virus	17	
2.4	o Botnet	17	
2.4	o Worm	17	
2.4	o Spyware	17	13.6, 13.10, 13.13
2.4	Tools and methods	17	
2.4	o Antivirus	17	
2.4	o Anti-malware	17	
2.4	o Recovery console	17	
2.4	o Backup/restore	17	
2.4	o End user education	17	
2.4	o Software firewalls	17	
2.4	o SecureDNS	17	
2.5	Compare and contrast social engineering, threats, and vulnerabilities.	16, 17	
2.5	Social engineering	17	
2.5	o Phishing	17	
2.5	o Spear phishing	17	

2.5	○ Impersonation	17	
2.5	○ Shoulder surfing	17	
2.5	○ Tailgating	17	
2.5	○ Dumpster diving	17	
2.5	DDoS	17	6.9, 13.6
2.5	DoS	17	
2.5	Zero-day	17	
2.5	Man-in-the-middle	17	
2.5	Brute force	16	
2.5	Dictionary	17	
2.5	Rainbow table	17	
2.5	Spoofing	17	
2.5	Non-compliant systems	17	
2.5	Zombie	17	
2.6	Compare and contrast the differences of basic Microsoft Windows OS security settings.	14, 16	
2.6	User and groups	16	
2.6	○ Administrator	16	
2.6	○ Power user	16	
2.6	○ Guest	16	
2.6	○ Standard user	16	
2.6	NTFS vs. share permissions	16	
2.6	○ Allow vs. deny	16	
2.6	○ Moving vs. copying folders and files	16	
2.6	○ File attributes	16	11.1, 11.2, 11.3, 11.4,
2.6	Shared files and folders	16	12.1, 12.5, 13.7, 13.8,
2.6	○ Administrative shares vs. local shares	16	
2.6	○ Permission propagation	16	
2.6	○ Inheritance	16	
2.6	System files and folders	16	
2.6	User authentication	16	
2.6	○ Single sign-on	16	
2.6	Run as administrator vs. standard user	14	
2.6	BitLocker	16	
2.6	BitLocker To Go	16	
2.6	EFS	16	
2.7	Given a scenario, implement security best practices to secure a workstation.	13, 16	
2.7	Password best practices	16	
2.7	○ Setting strong passwords	16	
2.7	○ Password expiration	16	
2.7	○ Screensaver required password	16	
2.7	○ BIOS/UEFI passwords	16	
2.7	○ Requiring passwords	16	
2.7	Account management	16	
2.7	○ Restricting user permissions	16	
2.7	○ Logon time restrictions	16	12.1, 12.4, 12.5, 12.10,
2.7	○ Disabling guest account	16	13.1, 13.3, 13.5, 13.7,
2.7	○ Failed attempts lockout	16	13.8, 13.9,
2.7	○ Timeout/screen lock	16	
2.7	○ Change default admin user account/password	16	
2.7	○ Basic Active Directory functions - Account creation	16	
2.7	○ Basic Active Directory functions - Account deletion	16	
2.7	○ Basic Active Directory functions - Password reset/unlock account	16	
2.7	○ Basic Active Directory functions - Disable account	16	
2.7	Disable autorun	16	
2.7	Data encryption	16	
2.7	Patch/update management	13	
2.8	Given a scenario, implement methods for securing mobile devices.	9	
2.8	Screen locks	9	
2.8	○ Fingerprint lock	9	

2.8	o Face lock	9	
2.8	o Swipe lock	9	
2.8	o Passcode lock Remote wipes	9	
2.8	Locator applications	9	
2.8	Remote backup applications	9	
2.8	Failed login attempts restrictions	9	
2.8	Antivirus/Anti-malware	9	9.7
2.8	Patching/OS updates	9	
2.8	Biometric authentication	9	
2.8	Full device encryption	9	
2.8	Multifactor authentication	9	
2.8	Authenticator applications	9	
2.8	Trusted sources vs. untrusted sources	9	
2.8	Firewalls	9	
2.8	Policies and procedures	9	
2.8	o BYOD vs. corporate-owned	9	
2.8	o Profile security requirements	9	
2.9	Given a scenario, implement appropriate data destruction and disposal methods.	17	
2.9	Physical destruction	17	
2.9	o Shredder	17	
2.9	o Drill/hammer	17	
2.9	o Electromagnetic (Degaussing)	17	13.3
2.9	o Incineration	17	
2.9	o Certificate of destruction	17	
2.9	Recycling or repurposing best practices	17	
2.9	o Low-level format vs. standard format	17	
2.9	o Overwrite	17	
2.9	o Drive wipe	17	
2.10	Given a scenario, configure security on SOHO wireless and wired networks.	7	
2.10	Wireless-specific	7	
2.10	o Changing default SSID	7	
2.10	o Setting encryption	7	
2.10	o Disabling SSID broadcast	7	
2.10	o Antenna and access point placement	7	
2.10	o Radio power levels	7	
2.10	o WPS	7	
2.10	Change default usernames and passwords	7	13.9
2.10	Enable MAC filtering	7	
2.10	Assign static IP addresses	7	
2.10	Firewall settings	7	
2.10	Port forwarding/mapping	7	
2.10	Disabling ports	7	
2.10	Content filtering/parental controls	7	
2.10	Update firmware	7	
2.10	Physical security	7	
3	Software Troubleshooting		
3.1	Given a scenario, troubleshoot Microsoft Windows OS problems.	13, 14, 15	
3.1	Common symptoms	14, 15	
3.1	o Slow performance	14	
3.1	o Limited connectivity	14	
3.1	o Failure to boot	15	
3.1	o No OS found	15	
3.1	o Application crashes	14	
3.1	o Blue screens	15	
3.1	o Black screens	15	
3.1	o Printing issues	14	
3.1	o Services fail to start	14	
3.1	o Slow bootup	14	
3.1	o Slow profile load	15	

3.1	Common solutions	13, 14, 15	4.0, 0.9, 0.10, 7.0, 0.0,
3.1	o Defragment the hard drive	13	10.2, 12.1, 12.11,
3.1	o Reboot	15	12.12, 12.14, 12.15,
3.1	o Kill tasks	14	13.6, 13.13
3.1	o Restart services	14	
3.1	o Update network settings	14	
3.1	o Reimage/reload OS	15	
3.1	o Roll back updates	15	
3.1	o Roll back devices drivers	15	
3.1	o Apply updates	15	
3.1	o Repair application	14	
3.1	o Update boot order	15	
3.1	o Disable Windows services/applications	14	
3.1	o Disable application startup	14	
3.1	o Safe boot	14	
3.1	o Rebuild Windows profiles	15	
3.2	Given a scenario, troubleshoot and resolve PC security issues.	17	
3.2	Common symptoms	17	
3.2	o Pop-ups	17	
3.2	o Browser redirection	17	
3.2	o Security alerts	17	
3.2	o Slow performance	17	
3.2	o Internet connectivity issues	17	
3.2	o PC/OS lockup	17	
3.2	o Application crash	17	
3.2	o OS updates failures	17	12.14, 13.13
3.2	o Rogue antivirus	17	
3.2	o Spam	17	
3.2	o Renamed system files	17	
3.2	o Disappearing files	17	
3.2	o File permission changes	17	
3.2	o Hijacked email - Responses from users regarding email	17	
3.2	o Hijacked email - Automated replies from unknown sent email	17	
3.2	o Access denied	17	
3.2	o Invalid certificate (trusted root CA)	17	
3.2	o System/application log errors	17	
3.3	Given a scenario, use best practice procedures for malware removal.	17	
3.3	1. Identify and research malware symptoms.	17	
3.3	2. Quarantine the infected systems.	17	
3.3	3. Disable System Restore (in Windows).	17	
3.3	4. Remediate the infected systems.	17	
3.3	a. Update the anti-malware software.	17	13.6
3.3	b. Scan and use removal techniques (safe mode, pre-installation environment).	17	
3.3	5. Schedule scans and run updates.	17	
3.3	6. Enable System Restore and create a restore point (in Windows).	17	
3.3	7. Educate the end user.	17	
3.4	Given a scenario, troubleshoot mobile OS and application issues.	9	
3.4	Common symptoms	9	
3.4	o Dim display	9	
3.4	o Intermittent wireless	9	
3.4	o No wireless connectivity	9	
3.4	o No Bluetooth connectivity	9	
3.4	o Cannot broadcast to external monitor	9	
3.4	o Touchscreen non-responsive	9	
3.4	o Apps not loading	9	
3.4	o Slow performance	9	9.8
3.4	o Unable to decrypt email	9	
3.4	o Extremely short battery life	9	
3.4	o Overheating	9	

3.4	o Frozen system	9	
3.4	o No sound from speakers	9	
3.4	o Inaccurate touch screen response	9	
3.4	o System lockout	9	
3.4	o App log errors	9	
3.5	Given a scenario, troubleshoot mobile OS and application security issues.	9	
3.5	Common symptoms	9	
3.5	o Signal drop/weak signal	9	
3.5	o Power drain	9	
3.5	o Slow data speeds	9	
3.5	o Unintended WiFi connection	9	
3.5	o Unintended Bluetooth pairing	9	9.7, 9.8
3.5	o Leaked personal files/data	9	
3.5	o Data transmission over limit	9	
3.5	o Unauthorized account access	9	
3.5	o Unauthorized location tracking	9	
3.5	o Unauthorized camera/microphone activation	9	
3.5	o High resource utilization	9	
4	Operational Procedures		
4.1	Compare and contrast best practices associated with types of documentation.	17	
4.1	Network topology diagrams	17	
4.1	Knowledge base/articles	17	
4.1	Incident documentation	17	2.6, 4.1, 13.1, 13.2, 13.3
4.1	Regulatory and compliance policy	17	
4.1	Acceptable use policy	17	
4.1	Password policy	17	
4.1	Inventory management	17	
4.1	o Asset tags	17	
4.1	o Barcodes	17	
4.2	Given a scenario, implement basic change management best practices.	17	
4.2	Documented business processes	17	
4.2	Purpose of the change	17	
4.2	Scope the change	17	
4.2	Risk analysis	17	2.3
4.2	Plan for change	17	
4.2	End-user acceptance	17	
4.2	Change board	17	
4.2	o Approvals Backout plan	17	
4.2	Document changes	17	
4.3	Given a scenario, implement basic disaster prevention and recovery methods.	13, 15	
4.3	Backup and recovery	13	
4.3	o Image level	13	
4.3	o File level	13	
4.3	o Critical applications	13	2.5, 9.7, 10.2, 12.11
4.3	Backup testing	13	
4.3	UPS	13	
4.3	Surge protector	13	
4.3	Cloud storage vs. local storage backups	13	
4.3	Account recovery options	15	
4.4	Explain common safety procedures.	Apx A	
4.4	Equipment grounding	Apx A	
4.4	Proper component handling and storage	Apx A	
4.4	o Antistatic bags	Apx A	
4.4	o ESD straps	Apx A	
4.4	o ESD mats	Apx A	
4.4	o Self-grounding	Apx A	
4.4	Toxic waste handling	Apx A	
4.4	o Batteries	Apx A	
4.4	o Toner	Apx A	

4.4	o CRT	Apx A	2.1
4.4	o Cell phones	Apx A	
4.4	o Tablets	Apx A	
4.4	Personal safety	Apx A	
4.4	o Disconnect power before repairing PC	Apx A	
4.4	o Remove jewelry	Apx A	
4.4	o Lifting techniques	Apx A	
4.4	o Weight limitations	Apx A	
4.4	o Electrical fire safety	Apx A	
4.4	o Cable management	Apx A	
4.4	o Safety goggles	Apx A	
4.4	o Air filter mask	Apx A	
4.4	Compliance with government regulations	Apx A	
4.5	Explain environmental impacts and appropriate controls.	Apx A	
4.5	MSDS documentation for handling and disposal	Apx A	
4.5	Temperature, humidity level awareness, and proper ventilation	Apx A	
4.5	Power surges, brownouts, and blackouts	Apx A	
4.5	o Battery backup	Apx A	
4.5	o Surge suppressor	Apx A	
4.5	Protection from airborne particles	Apx A	
4.5	o Enclosures	Apx A	
4.5	o Air filters/mask	Apx A	
4.5	Dust and debris	Apx A	
4.5	o Compressed air	Apx A	
4.5	o Vacuums	Apx A	
4.5	Compliance to government regulations	Apx A	
4.6	Explain the processes for addressing prohibited content/activity, and privacy, licensing, and policy concepts.	17	12.9, 13.1, 13.2, 13.4
4.6	Incident response	17	
4.6	o First response - Identify	17	
4.6	o First response - Report through proper channels	17	
4.6	o First response - Data/device preservation	17	
4.6	o Use of documentation/documentation changes	17	
4.6	o Chain of custody - Tracking of evidence/documenting process	17	
4.6	Licensing/DRM/EULA	17	
4.6	o Open-source vs. commercial license	17	
4.6	o Personal license vs. enterprise licenses	17	
4.6	Regulated data	17	
4.6	o PII	17	
4.6	o PCI	17	
4.6	o GDPR	17	
4.6	o PHI	17	
4.6	Follow all policies and security best practices	17	
4.7	Given a scenario, use proper communication techniques and professionalism.	11	
4.7	Use proper language and avoid jargon, acronyms, and slang, when applicable	11	
4.7	Maintain a positive attitude/project confidence	11	
4.7	Actively listen (taking notes) and avoid interrupting the customer	11	
4.7	Be culturally sensitive	11	
4.7	o Use appropriate professional titles, when applicable	11	
4.7	Be on time (if late, contact the customer)	11	
4.7	Avoid distractions	11	
4.7	o Personal calls	11	
4.7	o Texting/social media sites	11	
4.7	o Talking to coworkers while interacting with customers	11	
4.7	o Personal interruptions	11	
4.7	Dealing with difficult customers or situations	11	
4.7	o Do not argue with customers and/or be defensive	11	
4.7	o Avoid dismissing customer problems	11	
4.7	o Avoid being judgmental	11	

4.7	o Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding)	11	
4.7	o Do not disclose experiences via social media outlets	11	
4.7	Set and meet expectations/timeline and communicate status with the customer	11	
4.7	o Offer different repair/replacement options, if applicable	11	
4.7	o Provide proper documentation on the services provided	11	
4.7	o Follow up with customer/user at a later date to verify satisfaction	11	
4.7	Deal appropriately with customers' confidential and private materials	11	
4.7	o Located on a computer, desktop, printer, etc.	11	
4.8	Identify the basics of scripting.	18	
4.8	Script file types	18	
4.8	o .bat	18	
4.8	o .ps1	18	
4.8	o .vbs	18	
4.8	o .sh	18	
4.8	o .py	18	
4.8	o .js	18	1.4, 11.1, 11.2, 12.1, 12.14, 13.7
4.8	Environment variables	18	
4.8	Comment syntax	18	
4.8	Basic script constructs	18	
4.8	o Basic loops	18	
4.8	o Variables	18	
4.8	Basic data types	18	
4.8	o Integers	18	
4.8	o Strings	18	
4.9	Given a scenario, use remote access technologies.	18	
4.9	RDP	18	
4.9	Telnet	18	
4.9	SSH	18	
4.9	Third-party tools	18	6.5, 11.4, 12.6, 13.12
4.9	o Screen share feature	18	
4.9	o File share	18	
4.9	Security considerations of each access method	18	