TestOut

TestOut PC Pro – English 7.0.x

Objective Mappings:

TestOut PC Pro 7.0
CompTIA A+ 220-1101

CompTIA A+ 220-1102

Powered by LABSIM

Contents

This document contains six objective mappings. Click on a mapping to view its contents.

Objective Mapping: LabSim Section to TestOut PC Pro 7.0 Objectives

The TestOut PC Pro course covers the following TestOut PC Pro 7.0 exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	1.1 - Select and install PC components 1.1.2 - Install and connect a motherboard 1.5 - Configure networking devices 1.5.2 - Install and configure Internet connection devices
2.0	**PC Technician Responsibilities**	
2.1	Protection and Safety	
2.2	Environmental Controls	2.5 - Implement disaster prevention and recovery methods 2.5.3 - Install surge protection and a UPS
2.3	Professionalism	
2.4	Change Management	
2.5	PC Maintenance	

2.6	PC and Networking Tools	
2.7	Troubleshooting Process Overview	
2.8	Support Systems	2.2 - Use operating system features and utilities 2.2.4 - Manage applications and processes 4.4 - Use and configure a ticketing system 4.4.1 - Create a help ticket 4.4.2 - Close a help ticket 4.4.3 - Configure ticketing system settings
2.9	Documentation	3.3 - Implement security best practices 3.3.1 - Enforce password settings
3.0	**Hardware**	
3.1	Network Media	1.5 - Configure networking devices 1.5.1 - Install and configure wired and wireless network adapters and cables
3.2	Cables and Connectors	1.3 - Install and configure storage 1.3.1 - Install internal and external storage devices
3.3	Cases and Motherboards	1.1 - Select and install PC components

		1.1.2 - Install and connect a motherboard 1.1.3 - Install a CPU and CPU fan
3.4	Motherboard Troubleshooting	4.1 - Troubleshoot hardware components 4.1.1 - Troubleshoot system startup 4.1.2 - Troubleshoot system power 4.1.6 - Troubleshoot malfunctioning systems 4.4 - Use and configure a ticketing system 4.4.2 - Close a help ticket
3.5	Memory	1.1 - Select and install PC components 1.1.4 - Install memory modules
3.6	Memory Installation	1.1 - Select and install PC components 1.1.4 - Install memory modules
3.7	Memory Troubleshooting	4.1 - Troubleshoot hardware components 4.1.4 - Troubleshoot system memory
3.8	BIOS/UEFI	1.2 - Configure hardware components 1.2.2 - Configure BIOS/UEFI settings 1.2.3 - Implement firmware updates

		3.3 - Implement security best practices
		3.3.7 - Configure BIOS/UEFI security settings
3.9	Processors	1.1 - Select and install PC components
		1.1.3 - Install a CPU and CPU fan
3.10	Processor Troubleshooting	4.1 - Troubleshoot hardware components
		4.1.3 - Troubleshoot CPU installation
3.11	Video and Expansion Cards	1.1 - Select and install PC components
		1.1.5 - Select and install expansion cards
3.12	Audio	1.1 - Select and install PC components
		1.1.5 - Select and install expansion cards
3.13	Cooling	
3.14	Power Supplies	1.1 - Select and install PC components
		1.1.1 - Install and connect a power supply
4.0	**Operating Systems Basics**	
4.1	Operating System	2.1 - Install, update, and configure an operating system

		2.1.1 - Install, update, and configure Windows 2.1.2 - Install, update, and configure macOS 2.1.3 - Install, update, and configure Linux
4.2	Windows Basics	2.1 - Install, update, and configure an operating system 2.1.1 - Install, update, and configure Windows 2.1.3 - Install, update, and configure Linux
4.3	Linux Basics	2.1 - Install, update, and configure an operating system 2.1.3 - Install, update, and configure Linux 2.2 - Use operating system features and utilities 2.2.3 - Use common Linux command line utilities
4.4	macOS Basics	2.1 - Install, update, and configure an operating system 2.1.2 - Install, update, and configure macOS 2.2 - Use operating system features and utilities 2.2.2 - Use core macOS or iOS features
5.0	**Storage**	
5.1	Storage Devices	
5.2	SATA	1.3 - Install and configure storage

		1.3.1 - Install internal and external storage devices
5.3	Optical Media	
5.4	RAID	1.3 - Install and configure storage 1.3.3 - Implement a RAID solution
5.5	File Systems	1.3 - Install and configure storage 1.3.2 - Configure and manage storage 4.4 - Use and configure a ticketing system 4.4.2 - Close a help ticket
5.6	Storage Management	1.3 - Install and configure storage 1.3.2 - Configure and manage storage 1.3.4 - Perform disk maintenance
5.7	Storage Spaces	1.3 - Install and configure storage 1.3.2 - Configure and manage storage
5.8	Disk Optimization	1.3 - Install and configure storage 1.3.4 - Perform disk maintenance

5.9	Storage and RAID Troubleshooting	4.1 - Troubleshoot hardware components
		4.1.5 - Troubleshoot storage devices
6.0	**System Implementation**	
6.1	Windows Pre-Installation	2.1 - Install, update, and configure an operating system
		2.1.1 - Install, update, and configure Windows
6.2	Windows Installation	2.1 - Install, update, and configure an operating system
		2.1.1 - Install, update, and configure Windows
		4.4 - Use and configure a ticketing system
		4.4.2 - Close a help ticket
6.3	Cloud Computing	
6.4	Virtualization	2.7 - Configure virtualization
		2.7.2 - Install and configure a hypervisor 2.7.3 - Install and configure a virtual machine 2.7.4 - Create and add virtual hard disks
7.0	**System Management 1**	
7.1	Windows System Tools	2.2 - Use operating system features and utilities

		2.2.1 - Use Windows features and command line utilities
7.2	Windows Settings	
7.3	Performance Monitoring	
7.4	Windows Application Management	2.2 - Use operating system features and utilities 2.2.4 - Manage applications and processes
7.5	Linux Application Management	2.1 - Install, update, and configure an operating system 2.1.3 - Install, update, and configure Linux 2.2 - Use operating system features and utilities 2.2.3 - Use common Linux command line utilities
7.6	Digital Content Management	
7.7	Virtual Memory	2.3 - Manage file systems 2.3.1 - Manage files and folders
7.8	Windows and Application Troubleshooting	4.2 - Troubleshoot software components 4.2.1 - Troubleshoot common issues
7.9	Scripting Basics	

8.0	System Management 2	

8.1	Active Directory	2.1 - Install, update, and configure an operating system
		
		    2.1.7 - Configure local users and groups
		
		2.2 - Use operating system features and utilities
		
		    2.2.1 - Use Windows features and command line utilities
		
		2.4 - Configure PC networking
		
		    2.4.2 - Configure Windows workgroup or domain settings

8.2	Users and Groups	2.1 - Install, update, and configure an operating system 2.1.7 - Configure local users and groups
8.3	Remote Services	2.6 - Implement remote access 2.6.1 - Configure Remote Desktop Connection
8.4	VPN	2.6 - Implement remote access 2.6.2 - Configure a VPN connection

8.5	Updates	2.1 - Install, update, and configure an operating system
		
		    2.1.1 - Install, update, and configure Windows
		    2.1.2 - Install, update, and configure macOS

		2.1.3 - Install, update, and configure Linux
		3.1 - Implement tools to detect, remove, and prevent malware
		3.1.4 - Configure operating system updates
8.6	System Backup	**2.5 - Implement disaster prevention and recovery methods**
		2.5.1 - Implement image-level backup and recovery
		2.5.2 - Implement file-level backup and recovery
		4.4 - Use and configure a ticketing system
		4.4.2 - Close a help ticket
8.7	System Recovery	**2.5 - Implement disaster prevention and recovery methods**
		2.5.1 - Implement image-level backup and recovery
		2.5.2 - Implement file-level backup and recovery
		3.1 - Implement tools to detect, remove, and prevent malware
		3.1.2 - Restore a PC or mobile device
		4.2 - Troubleshoot software components
		4.2.1 - Troubleshoot common issues
8.8	Windows Boot Errors	**1.2 - Configure hardware components**
		1.2.1 - Configure boot options

		1.2.2 - Configure BIOS/UEFI settings
		2.1 - Install, update, and configure an operating system
		2.1.1 - Install, update, and configure Windows
		2.2 - Use operating system features and utilities
		2.2.1 - Use Windows features and command line utilities
		4.1 - Troubleshoot hardware components
		4.1.1 - Troubleshoot system startup
		4.1.6 - Troubleshoot malfunctioning systems
		4.2 - Troubleshoot software components
		4.2.1 - Troubleshoot common issues
9.0	**File Management**	
9.1	Manage Files on Windows	2.2 - Use operating system features and utilities
		2.2.1 - Use Windows features and command line utilities
		2.3 - Manage file systems
		2.3.1 - Manage files and folders
		2.3.2 - Configure file access permissions
9.2	NTFS and Share Permissions	2.3 - Manage file systems
		2.3.1 - Manage files and folders

		2.3.2 - Configure file access permissions 2.3.3 - Share and secure files and folders
9.3	File Encryption	2.3 - Manage file systems 2.3.3 - Share and secure files and folders 3.3 - Implement security best practices 3.3.4 - Implement drive encryption
9.4	Linux File Management	2.2 - Use operating system features and utilities 2.2.3 - Use common Linux command line utilities
10.0	**Peripheral Devices**	
10.1	Peripheral Devices	
10.2	Display Devices	2.1 - Install, update, and configure an operating system 2.1.5 - Configure and optimize video adapter settings
10.3	Display, Video, and Projector Troubleshooting	2.1 - Install, update, and configure an operating system 2.1.5 - Configure and optimize video adapter settings
10.4	Device Driver Management	2.1 - Install, update, and configure an operating system

		2.1.4 - Manage device drivers **2.2 - Use operating system features and utilities** 2.2.3 - Use common Linux command line utilities
10.5	Device Driver Troubleshooting	**1.2 - Configure hardware components** 1.2.1 - Configure boot options 1.2.2 - Configure BIOS/UEFI settings 1.2.3 - Implement firmware updates **2.1 - Install, update, and configure an operating system** 2.1.4 - Manage device drivers
11.0	**Networking**	
11.1	Networking Overview	
11.2	Networking Ports and Protocols	
11.3	Client-Side Network Configuration	**2.4 - Configure PC networking** 2.4.1 - Configure client IP addressing, DNS, and DHCP 2.4.3 - Configure wired and wireless networking for a SOHO
11.4	Services Provided by Network Devices	**1.5 - Configure networking devices** 1.5.2 - Install and configure Internet connection devices

		2.3 - Manage file systems	
		2.3.1 - Manage files and folders	
		2.4 - Configure PC networking	
		2.4.1 - Configure client IP addressing, DNS, and DHCP 2.4.4 - Use network utilities	
11.5	Wireless Networking	1.5 - Configure networking devices	
		1.5.1 - Install and configure wired and wireless network adapters and cables	
		2.4 - Configure PC networking	
		2.4.3 - Configure wired and wireless networking for a SOHO	
11.6	SOHO Configuration	1.2 - Configure hardware components	
		1.2.3 - Implement firmware updates	
		2.4 - Configure PC networking	
		2.4.3 - Configure wired and wireless networking for a SOHO	
11.7	Networking Hardware	1.5 - Configure networking devices	
		1.5.1 - Install and configure wired and wireless network adapters and cables	

		2.4 - Configure PC networking 2.4.3 - Configure wired and wireless networking for a SOHO

11.8	Command Line Network Utilities	2.2 - Use operating system features and utilities
		
		    2.2.1 - Use Windows features and command line utilities
		    2.2.3 - Use common Linux command line utilities

11.9	Network Troubleshooting	4.3 - Troubleshoot networking
		
		    4.3.1 - Troublehsoot a network connection
		    4.3.2 - Use networking utilities to view, test, and troubleshoot network configuration, communication, and connectivity issues
		
		4.4 - Use and configure a ticketing system
		
		    4.4.1 - Create a help ticket
		    4.4.2 - Close a help ticket

12.0	**Mobile Devices**	

12.1	Laptops	1.6 - Manage mobile devices
		
		    1.6.1 - Install basic hardware components on laptop computers
		    1.6.3 - Use common mobile device features

12.2	Mobile Device Displays and Components	1.6 - Manage mobile devices 1.6.1 - Install basic hardware components on laptop computers

12.3	Laptop Power Management	2.2 - Use operating system features and utilities
		2.2.5 - Configure power options and settings
		4.1 - Troubleshoot hardware components
		4.1.2 - Troubleshoot system power
12.4	Mobile Devices	1.6 - Manage mobile devices
		1.6.2 - Configure mobile device connectivity
		1.6.3 - Use common mobile device features
12.5	Mobile Device Network Connectivity	1.6 - Manage mobile devices
		1.6.2 - Configure mobile device connectivity
		1.6.3 - Use common mobile device features
		3.2 - Implement mobile device security
		3.2.1 - Implement access control and authentication
12.6	Mobile Device Security	3.2 - Implement mobile device security
		3.2.1 - Implement access control and authentication
		3.2.2 - Implement device encryption
		3.2.3 - Implement device location
		3.2.4 - Implement remote wipe capabilities
12.7	Laptop and Mobile Device Troubleshooting	1.6 - Manage mobile devices

		1.6.3 - Use common mobile device features
		
		4.1 - Troubleshoot hardware components
		
		    4.1.6 - Troubleshoot malfunctioning systems
		    4.1.7 - Troubleshoot mobile devices
		
		4.3 - Troubleshoot networking
		
		    4.3.1 - Troublehsoot a network connection

13.0	**Printing**	

13.1	Printer Overview	1.4 - Install and configure a printer
		
		    1.4.1 - Select and install a printer
		    1.4.2 - Configure printer properties
		    1.4.4 - Manage printing
		
		3.3 - Implement security best practices
		
		    3.3.1 - Enforce password settings
		
		4.1 - Troubleshoot hardware components
		
		    4.1.8 - Troubleshoot printer issues
		
		4.2 - Troubleshoot software components
		
		    4.2.2 - Apply common solutions
		
		4.4 - Use and configure a ticketing system

		4.4.2 - Close a help ticket

13.2	Print Connectivity	1.4 - Install and configure a printer
		
		    1.4.1 - Select and install a printer
		    1.4.2 - Configure printer properties
		    1.4.3 - Configure network printing
		    1.4.4 - Manage printing
		
		1.5 - Configure networking devices
		
		    1.5.2 - Install and configure Internet connection devices
		
		2.3 - Manage file systems
		
		    2.3.1 - Manage files and folders
		    2.3.2 - Configure file access permissions
		    2.3.3 - Share and secure files and folders
		
		3.2 - Implement mobile device security
		
		    3.2.1 - Implement access control and authentication
		
		3.3 - Implement security best practices
		
		    3.3.1 - Enforce password settings
		
		4.1 - Troubleshoot hardware components
		
		    4.1.8 - Troubleshoot printer issues

13.3	Printer Types and Components	1.4 - Install and configure a printer

		1.4.4 - Manage printing **4.1 - Troubleshoot hardware components** 4.1.8 - Troubleshoot printer issues
13.4	Printer Troubleshooting	**4.1 - Troubleshoot hardware components** 4.1.8 - Troubleshoot printer issues
14.0	**Security**	
14.1	Security Best Practices	**3.3 - Implement security best practices** 3.3.1 - Enforce password settings 3.3.2 - Require a screen saver password
14.2	Incident Response and Regulated Data	
14.3	Physical Security	
14.4	Logical Security Measures	**3.3 - Implement security best practices** 3.3.1 - Enforce password settings 3.3.2 - Require a screen saver password 3.3.3 - Manage Linux passwords
14.5	Social Engineering Attacks	
14.6	Data Destruction and Disposal	**3.2 - Implement mobile device security**

		3.2.4 - Implement remote wipe capabilities
14.7	Malware Protection	3.1 - Implement tools to detect, remove, and prevent malware 3.1.1 - Install and configure anti-virus and anti-malware utilities
14.8	Firewalls	3.3 - Implement security best practices 3.3.5 - Configure a firewall
14.9	Proxy Servers	3.3 - Implement security best practices 3.3.6 - Use a proxy server
14.10	Install, Configure, and Secure Browsers	
14.11	Security Troubleshooting	4.2 - Troubleshoot software components 4.2.1 - Troubleshoot common issues 4.2.2 - Apply common solutions
15.0	**Capstone Exercises**	
		1.1 - Select and install PC components 1.1.1 - Install and connect a power supply 1.1.2 - Install and connect a motherboard 1.1.3 - Install a CPU and CPU fan 1.1.4 - Install memory modules 1.1.5 - Select and install expansion cards

1.2 - Configure hardware components

1.2.1 - Configure boot options
1.2.2 - Configure BIOS/UEFI settings

1.3 - Install and configure storage

1.3.3 - Implement a RAID solution

1.5 - Configure networking devices

1.5.1 - Install and configure wired and wireless network adapters and cables

2.2 - Use operating system features and utilities

2.2.1 - Use Windows features and command line utilities
2.2.3 - Use common Linux command line utilities
2.2.4 - Manage applications and processes

2.3 - Manage file systems

2.3.1 - Manage files and folders
2.3.2 - Configure file access permissions
2.3.3 - Share and secure files and folders

3.2 - Implement mobile device security

3.2.1 - Implement access control and authentication

3.3 - Implement security best practices

3.3.7 - Configure BIOS/UEFI security settings

		4.1 - Troubleshoot hardware components 4.1.1 - Troubleshoot system startup 4.1.2 - Troubleshoot system power
A.0	**TestOut PC Pro - Practice Exams**	
A.1	Prepare for TestOut PC Pro Certification	
A.2	TestOut PC Pro Exam Domain Review	
A.3	TestOut PC Pro Certification Practice Exam	
B.0	**CompTIA A+ Core 1 (220-1101) - Practice Exams**	
B.1	Prepare for CompTIA A+ Core 1 (220-1101) Certification	
B.2	CompTIA A+ Core 1 (220-1101) Domain Review (20 Questions)	
B.3	CompTIA A+ Core 1 (220-1101) Domain Review (All Questions)	
C.0	**CompTIA A+ Core 2 (220-1102) - Practice Exams**	
C.1	Prepare for CompTIA A+ Core 2 (220-1102) Certification	

C.2	CompTIA A+ Core 2 (220-1102) Domain Review (20 Questions)	
C.3	CompTIA A+ Core 2 (220-1102) Domain Review (All Questions)	

Objective Mapping: TestOut PC Pro 7.0 Objectives to LabSim Section

The TestOut PC Pro course and certification exam cover the following TestOut PC Pro 7.0 objectives:

#	Domain	Module.Section
1.0	**Hardware**	
1.1	Select and install PC components 1.1.1 - Install and connect a power supply 1.1.2 - Install and connect a motherboard 1.1.3 - Install a CPU and CPU fan 1.1.4 - Install memory modules 1.1.5 - Select and install expansion cards	1.1 3.3, 3.5, 3.6, 3.9, 3.11, 3.12, 3.14 14.11
1.2	Configure hardware components 1.2.1 - Configure boot options 1.2.2 - Configure BIOS/UEFI settings 1.2.3 - Implement firmware updates	3.8 8.8 10.5 11.6 14.11
1.3	Install and configure storage 1.3.1 - Install internal and external storage devices 1.3.2 - Configure and manage storage 1.3.3 - Implement a RAID solution 1.3.4 - Perform disk maintenance	3.2 5.2, 5.4, 5.5, 5.6, 5.7, 5.8 14.11

1.4	Install and configure a printer	13.1, 13.2, 13.3
	1.4.1 - Select and install a printer 1.4.2 - Configure printer properties 1.4.3 - Configure network printing 1.4.4 - Manage printing	
1.5	Configure networking devices	1.1 3.1 11.4, 11.5, 11.7 13.2 14.11
	1.5.1 - Install and configure wired and wireless network adapters and cables 1.5.2 - Install and configure Internet connection devices	
1.6	Manage mobile devices	12.1, 12.2, 12.4, 12.5, 12.7
	1.6.1 - Install basic hardware components on laptop computers 1.6.2 - Configure mobile device connectivity 1.6.3 - Use common mobile device features	
2.0	**Software**	
2.1	Install, update, and configure an operating system	4.1, 4.2, 4.3, 4.4 6.1, 6.2 7.5 8.1, 8.2, 8.5, 8.8 10.2, 10.3, 10.4, 10.5
	2.1.1 - Install, update, and configure Windows 2.1.2 - Install, update, and configure macOS 2.1.3 - Install, update, and configure Linux 2.1.4 - Manage device drivers 2.1.5 - Configure and optimize video adapter settings 2.1.6 - Manage audio device settings 2.1.7 - Configure local users and groups	

2.2	Use operating system features and utilities	2.8
		4.3, 4.4
	2.2.1 - Use Windows features and command line utilities	7.1, 7.4, 7.5
	2.2.2 - Use core macOS or iOS features	
	2.2.3 - Use common Linux command line utilities	8.1, 8.8
	2.2.4 - Manage applications and processes	
	2.2.5 - Configure power options and settings	9.1, 9.4
		10.4
		11.8
		12.3
		14.11
2.3	Manage file systems	7.7
		9.1, 9.2, 9.3
	2.3.1 - Manage files and folders	11.4
	2.3.2 - Configure file access permissions	
	2.3.3 - Share and secure files and folders	13.2
		14.11
2.4	Configure PC networking	8.1
		11.3, 11.4, 11.5, 11.6, 11.7
	2.4.1 - Configure client IP addressing, DNS, and DHCP	
	2.4.2 - Configure Windows workgroup or domain settings	
	2.4.3 - Configure wired and wireless networking for a SOHO	
	2.4.4 - Use network utilities	
	2.4.5 - Configure network drive mappings	
2.5	Implement disaster prevention and recovery methods	2.2
		8.6, 8.7
	2.5.1 - Implement image-level backup and recovery	

	2.5.2 - Implement file-level backup and recovery 2.5.3 - Install surge protection and a UPS	
2.6	Implement remote access 2.6.1 - Configure Remote Desktop Connection 2.6.2 - Configure a VPN connection	8.3, 8.4
2.7	Configure virtualization 2.7.1 - Enable hardware virtualization in BIOS/UEFI 2.7.2 - Install and configure a hypervisor 2.7.3 - Install and configure a virtual machine 2.7.4 - Create and add virtual hard disks	6.4
3.0	**Security**	
3.1	Implement tools to detect, remove, and prevent malware 3.1.1 - Install and configure anti-virus and anti-malware utilities 3.1.2 - Restore a PC or mobile device 3.1.3 - Recover files corrupted by malware 3.1.4 - Configure operating system updates	8.5, 8.7 14.7
3.2	Implement mobile device security 3.2.1 - Implement access control and authentication 3.2.2 - Implement device encryption 3.2.3 - Implement device location 3.2.4 - Implement remote wipe capabilities	12.5, 12.6 13.2 14.6 14.11

3.3	Implement security best practices	2.9
		3.8
	3.3.1 - Enforce password settings	9.3
	3.3.2 - Require a screen saver password	
	3.3.3 - Manage Linux passwords	13.1, 13.2
	3.3.4 - Implement drive encryption	
	3.3.5 - Configure a firewall	14.1, 14.4, 14.8, 14.9
	3.3.6 - Use a proxy server	
	3.3.7 - Configure BIOS/UEFI security settings	14.11
4.0	**Troubleshooting**	
4.1	Troubleshoot hardware components	3.4, 3.7, 3.10
		5.9
	4.1.1 - Troubleshoot system startup	8.8
	4.1.2 - Troubleshoot system power	
	4.1.3 - Troubleshoot CPU installation	12.3, 12.7
	4.1.4 - Troubleshoot system memory	
	4.1.5 - Troubleshoot storage devices	13.1, 13.2, 13.3, 13.4
	4.1.6 - Troubleshoot malfunctioning systems	
	4.1.7 - Troubleshoot mobile devices	14.11
	4.1.8 - Troubleshoot printer issues	
4.2	Troubleshoot software components	7.8
		8.7, 8.8
	4.2.1 - Troubleshoot common issues	13.1
	4.2.2 - Apply common solutions	
		14.11
4.3	Troubleshoot networking	11.9
		12.7
	4.3.1 - Troubleshoot a network connection	

		4.3.2 - Use networking utilities to view, test, and troubleshoot network configuration, communication, and connectivity issues	
4.4	Use and configure a ticketing system 4.4.1 - Create a help ticket 4.4.2 - Close a help ticket 4.4.3 - Configure ticketing system settings		2.8 3.4 5.5 6.2 8.6 11.9 13.1

Objective Mapping: LabSim Section to CompTIA 220-1101 Objectives

The TestOut PC Pro course covers the following CompTIA A+ Certification 220-1101 exam objectives:

Section	Title	Objectives
1.0	**Course Introduction**	
1.1	Course Introduction	1.1 - Given a scenario, install and configure laptop hardware and components. 1.1.1 - Hardware/device replacement 1.1.1.2 - Keyboard/keys 1.1.1.3 - Random-access memory (RAM) 1.1.1.4 - Hard disk drive (HDD)/solid-state drive (SSD) migration 1.1.1.5 - HDD/SSD replacement 2.2 - Compare and contrast common networking hardware. 2.2.1 - Routers 2.2.4 - Patch panel 3.3 - Given a scenario, select and install storage devices. 3.3.4 - Removable storage 3.3.4.1 - Flash drives 3.3.4.2 - Memory cards 3.3.4.3 - Optical drives
2.0	**PC Technician Responsibilities**	

2.1	Protection and Safety	
2.2	Environmental Controls	
2.3	Professionalism	
2.4	Change Management	
2.5	PC Maintenance	1.1 - Given a scenario, install and configure laptop hardware and components. 1.1.1 - Hardware/device replacement 3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.8 - Cooling 3.4.8.1 - Fans 3.7 - Given a scenario, install and replace printer consumables. 3.7.2 - Inkjet 3.7.2.3 Maintenance: Clean heads, replace cartridges, calibrate, clear jams 5.4 - Given a scenario, troubleshoot video, projector, and display issues. 5.4.1 - Common symptoms 5.4.1.2 - Physical cabling issues

		5.7 - Given a scenario, troubleshoot problems with wired and wireless networks. 5.7.1 - Common symptoms 5.7.1.8 - External interference
2.6	PC and Networking Tools	2.8 - Given a scenario, use networking tools. 2.8.1 - Crimper 2.8.2 - Cable stripper 2.8.3 - WiFi analyzer 2.8.4 - Toner probe 2.8.5 - Punchdown tool 2.8.6 - Cable tester 2.8.7 - Loopback plug 2.8.8 - Network tap 5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power. 5.2.1 - Common symptoms 5.2.1.4 - No power

2.7	Troubleshooting Process Overview	5.1 - Given a scenario, apply the best practice methodology to resolve problems.
		
		5.1.1 - Always consider corporate policies, procedures, and impacts before implementing changes
		
		5.1.1.1 - 1. Identify the problem
		    o 5.1.1.1.1 - Gather information from the user, identify user changes, and, if applicable, perform backups before making changes
		    o 5.1.1.1.2 - Inquire regarding environmental or infrastructure changes

		5.1.1.2 - 2. Establish a theory of probable cause (question the obvious)
		    ○ 5.1.1.2.1 - If necessary, conduct external or internal research based on symptoms
		5.1.1.3 - 3. Test the theory to determine the cause
		    ○ 5.1.1.3.1 - Once the theory is confirmed, determine the next steps to resolve the problem
		    ○ 5.1.1.3.2 - If the theory is not confirmed, re-establish a new theory or escalate
		5.1.1.4 - 4. Establish a plan of action to resolve the problem and implement the solution
		    ○ 5.1.1.4.1 - Refer to the vendor's instructions for guidance
		5.1.1.5 - 5. Verify full system functionality and, if applicable, implement preventive measures
		5.1.1.6 - 6. Document the findings, actions, and outcomes

2.8	Support Systems	
2.9	Documentation	
3.0	**Hardware**	

3.1	Network Media	3.1 - Explain basic cable types and their connectors, features, and purposes.
		
		3.1.1 - Network cables
		
		3.1.1.1 - Copper
		3.1.1.1.1 - Cat 5
		3.1.1.1.2 - Cat 5e
		    ○ 3.1.1.1.3 - Cat 6
		    ○ 3.1.1.1.4 - Cat 6a
		    ○ 3.1.1.1.5 - Coaxial
		    ○ 3.1.1.1.6 - Shielded twisted pair
		        ▪ 3.1.1.1.6.1 - Direct burial
		    ○ 3.1.1.1.7 - Unshielded twisted pair

<table>
<tr>
<td></td>
<td></td>
<td>

3.1.1.2 - Plenum
3.1.1.3 - Optical
         o   3.1.1.3.1 - Fiber
3.1.1.4 - T568A/T568B

3.1.6 - Connector types

    3.1.6.1 - RJ11
    3.1.6.2 - RJ45
    3.1.6.3 - F type
    3.1.6.4 - Straight tip (ST)
    3.1.6.5 - Subscriber connector (SC)
    3.1.6.6 - Lucent connector (LC)
    3.1.6.7 - Punchdown block
</td>
</tr>
<tr>
<td>3.2</td>
<td>Cables and Connectors</td>
<td>

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

3.1.2 - Peripheral cables

    3.1.2.1 - USB 2.0
    3.1.2.2 - USB 3.0
    3.1.2.3 - Serial
    3.1.2.4 - Thunderbolt

3.1.3 - Video cables

    3.1.3.1 - High-Definition Multimedia Interface (HDMI)
    3.1.3.2 - DisplayPort
    3.1.3.3 - Digital Visual Interface (DVI)
    3.1.3.4 - Video Graphics Array (VGA)

3.1.4 - Hard drive cables

    3.1.4.1 - Serial Advanced Technology Attachment (SATA)
    3.1.4.2 - Small Computer System Interface (SCSI)
</td>
</tr>
</table>

		3.1.4.3 - External SATA (eSATA) 3.1.4.4 - Integrated Drive Electronics (IDE) 3.1.5 - Adapters 3.1.6 - Connector types 3.1.6.1 - RJ11 3.1.6.2 - RJ45 3.1.6.8 - microUSB 3.1.6.9 - miniUSB 3.1.6.10 - USB-C 3.1.6.11 - Molex 3.1.6.12 - Lightning port 3.1.6.13 - DB9 3.6 - Given a scenario, deploy and configure multifunction devices/printers and settings. 3.6.3 - Device connectivity 3.6.3.1 - USB
3.3	Cases and Motherboards	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.1 - Motherboard form factor 3.4.1.1 - Advanced Technology eXtended (ATX) 3.4.1.2 - Information Technology eXtended (ITX) 3.4.2 - Motherboard connector types 3.4.2.1 - Peripheral Component Interconnect (PCI) 3.4.2.2 - PCI Express (PCIe) 3.4.2.3 - Power connectors 3.4.2.4 - SATA

		3.4.2.6 - SAN 3.4.2.7 - Headers 3.4.2.8 - M.2 3.4.3 - Motherboard compatibility 3.4.3.1 - CPU sockets 3.4.4 - Basic Input/Output System (BIOS)/Unified Extemsible Firmware Interface (UEFI) settings 3.4.7 - Expansion cards 3.4.8 - Cooling 3.4.8.1 - Fans
3.4	Motherboard Troubleshooting	5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power. 5.2.1 - Common symptoms 5.2.1.1 - Power-on self-test (POST) beeps 5.2.1.2 - Proprietary crash screens (blue screen of death [BSOD]/pinwheel) 5.2.1.3 - Black screen 5.2.1.4 - No power 5.2.1.5 - Sluggish performance 5.2.1.6 - Overheating 5.2.1.7 - Burning smell 5.2.1.8 - Intermittent shutdown 5.2.1.9 - Application crashes 5.2.1.10 - Grinding noise 5.2.1.11 - Capacitor swelling 5.2.1.12 - Inaccurate system date/time
3.5	Memory	3.2 - Given a scenario, install the appropriate RAM.

		3.2.1 - RAM types
		
		    3.2.1.2 - Small outline dual inline memory module (SODIMM)
		    3.2.1.3 - Double Data Rate 3 (DDR3)
		    3.2.1.4 - Double Data Rate 4 (DDR4)
		    3.2.1.5 - Double Data Rate 5 (DDR5)
		    3.2.1.6 - Error correction code (ECC) RAM
		
		3.2.2 - Single-channel
		3.2.3 - Dual-channel
		3.2.4 - Triple-channel
		3.2.5 - Quad-channel

3.6	Memory Installation	3.2 - Given a scenario, install the appropriate RAM.
		
		3.2.1 - RAM types
		
		    3.2.1.3 - Double Data Rate 3 (DDR3)
		    3.2.1.4 - Double Data Rate 4 (DDR4)
		    3.2.1.6 - Error correction code (ECC) RAM
		
		3.2.2 - Single-channel
		3.2.3 - Dual-channel
		3.2.4 - Triple-channel
		3.2.5 - Quad-channel

3.7	Memory Troubleshooting	5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.
		
		5.2.1 - Common symptoms
		
		    5.2.1.1 - Power-on self-test (POST) beeps
		    5.2.1.3 - Black screen
		    5.2.1.5 - Sluggish performance
		    5.2.1.8 - Intermittent shutdown

		5.2.1.9 - Application crashes

3.8	BIOS/UEFI	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
		
		3.4.4 - Basic Input/Output System (BIOS)/Unified Extemsible Firmware Interface (UEFI) settings
		
		    3.4.4.1 - Boot options
		    3.4.4.2 - USB permissions
		    3.4.4.3 - Trusted Platform Module (TPM) security features
		    3.4.4.5 - Secure Boot
		    3.4.4.6 - Boot password
		
		3.4.5 - Encryption
		3.4.6 - CPU architecture
		
		    3.4.6.4 - Multicore
		    3.4.6.5 - Multithreading
		    3.4.6.6 - Virtualization support

3.9	Processors	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
		
		3.4.3 - Motherboard compatibility
		
		    3.4.3.1 - CPU sockets
		    3.4.3.1.1 - Advanced Micro Devices, Inc. (AMD)
		    3.4.3.1.2 - Intel
		    3.4.3.3 - Multisocket
		
		3.4.6 - CPU architecture
		
		    3.4.6.1 - x64/x86

		3.4.6.3 - Single-core 3.4.6.4 - Multicore 3.4.6.5 - Multithreading 3.4.6.6 - Virtualization support 3.4.8 - Cooling 3.4.8.1 - Fans 3.4.8.2 - Heat sink 3.4.8.3 - Thermal paste/pads 3.4.8.4 - Liquid
3.10	Processor Troubleshooting	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.3 - Motherboard compatibility 3.4.3.1 - CPU sockets 5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power. 5.2.1 - Common symptoms 5.2.1.1 - Power-on self-test (POST) beeps 5.2.1.3 - Black screen 5.2.1.4 - No power 5.2.1.6 - Overheating 5.2.1.8 - Intermittent shutdown
3.11	Video and Expansion Cards	3.1 - Explain basic cable types and their connectors, features, and purposes. 3.1.3 - Video cables 3.1.3.1 - High-Definition Multimedia Interface (HDMI)

		3.1.3.2 - DisplayPort
		3.1.3.3 - Digital Visual Interface (DVI)
		3.1.3.4 - Video Graphics Array (VGA)
		
		3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
		
		   3.4.2 - Motherboard connector types
		
		      3.4.2.1 - Peripheral Component Interconnect (PCI)
		      3.4.2.2 - PCI Express (PCIe)
		
		   3.4.7 - Expansion cards
		
		      3.4.7.2 - Video card
		      3.4.7.3 - Capture card

3.12	Audio	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
		
		   3.4.7 - Expansion cards
		
		      3.4.7.1 - Sound card

3.13	Cooling	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.8 - Cooling
3.14	Power Supplies	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.

3.4.1 - Motherboard form factor

3.4.1.1 - Advanced Technology eXtended (ATX)
3.4.1.2 - Information Technology eXtended (ITX)

3.4.2 - Motherboard connector types

3.4.2.3 - Power connectors

3.4.3 - Motherboard compatibility

3.4.3.1 - CPU sockets

3.4.3.1.1 - Advanced Micro Devices, Inc. (AMD)

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

3.5.1 - Input 115V vs. 220V
3.5.2 - Output 3.3V vs. 5V vs. 12V
3.5.3 - 20-pin to 24-pin motherboard adapter
3.5.4 - Redundant power supply
3.5.5 - Modular power supply
3.5.6 - Wattage rating

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

5.2.1 - Common symptoms

5.2.1.4 - No power

| 4.0 | **Operating Systems Basics** | |

4.1	Operating System	
4.2	Windows Basics	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.6 - CPU architecture 3.4.6.5 - Multithreading
4.3	Linux Basics	
4.4	macOS Basics	
5.0	**Storage**	

5.1	Storage Devices	3.3 - Given a scenario, select and install storage devices.
		
		3.3.1 - Hard drives
		
		3.3.1.1 - Speeds
		   o 3.3.1.1.1 - 5,400rpm
		   o 3.3.1.1.2 - 7,200rpm
		   o 3.3.1.1.3 - 10,000rpm
		   o 3.3.1.1.4 - 15,000rpm
		3.3.1.2 - Form factor
		   o 3.3.1.2.1 - 2.5
		
		3.3.2 - SSDs
		
		3.3.2.1 - Communications interfaces
		   o 3.3.2.1.1 - Non-volatile Memory Express (NVMe)
		   o 3.3.2.1.2 - SATA
		   o 3.3.2.1.3 - Peripheral Component Interconnect Express (PCIe)

		3.3.2.2 - Form Factors
		    o 3.3.2.2.1 - M2
		    o 3.3.2.2.2 - mSATA
		
		3.3.4 - Removable storage
		
		3.3.4.1 - Flash drives
		3.3.4.2 - Memory cards
		3.3.4.3 - Optical drives

5.2	SATA	3.1 - Explain basic cable types and their connectors, features, and purposes. 3.1.4 - Hard drive cables 3.1.4.1 - Serial Advanced Technology Attachment (SATA) 3.1.4.3 - External SATA (eSATA) 3.3 - Given a scenario, select and install storage devices. 3.3.1 - Hard drives 3.3.1.2 - Form factor 3.3.1.2.1 - 2.5 3.3.1.2.2 - 3.5 3.3.2 - SSDs 3.3.2.1.2 - SATA 3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.2 - Motherboard connector types

		3.4.2.4 - SATA 3.4.2.5 - eSATA
5.3	Optical Media	3.3 - Given a scenario, select and install storage devices. 3.3.4 - Removable storage 3.3.4.3 - Optical drives 5.3 - Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays. 5.3.1 - Common symptoms 5.3.1.10 - Missing drives in OS
5.4	RAID	3.3 - Given a scenario, select and install storage devices. 3.3.3 - Drive configurations 3.3.3.1 - Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10
5.5	File Systems	
5.6	Storage Management	
5.7	Storage Spaces	3.3 - Given a scenario, select and install storage devices. 3.3.1 - Hard drives

5.8	Disk Optimization	1.1 - Given a scenario, install and configure laptop hardware and components.
		1.1.1 - Hardware/device replacement
		1.1.1.4 - Hard disk drive (HDD)/solid-state drive (SSD) migration 1.1.1.5 - HDD/SSD replacement
		3.3 - Given a scenario, select and install storage devices.
		3.3.1 - Hard drives

		3.3.1.1 - Speeds
		   o 3.3.1.1.1 - 5,400rpm
		   o 3.3.1.1.2 - 7,200rpm
		   o 3.3.1.1.3 - 10,000rpm
		   o 3.3.1.1.4 - 15,000rpm

		3.3.2 - SSDs
		3.3.2.1.1 - Non-volatile Memory Express (NVMe) 3.3.2.1.2 - SATA 3.3.2.1.3 - Peripheral Component Interconnect Express (PCIe) 3.3.2.2.1 - M2
5.9	Storage and RAID Troubleshooting	3.3 - Given a scenario, select and install storage devices.
		3.3.2 - SSDs
		5.3 - Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.
		5.3.1 - Common symptoms
		5.3.1.2 - Grinding noises 5.3.1.3 - Clicking sounds 5.3.1.4 - Bootable device not found

		5.3.1.5 - Data loss/corruption 5.3.1.6 - RAID failure 5.3.1.7 - Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T) failure 5.3.1.9 - Input/output operations per second (IOPS) 5.3.1.10 - Missing drives in OS
6.0	**System Implementation**	
6.1	Windows Pre-Installation	
6.2	Windows Installation	3.3 - Given a scenario, select and install storage devices. 3.3.3 - Drive configurations 3.3.3.1 - Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10
6.3	Cloud Computing	4.1 - Summarize cloud-computing concepts. 4.1.1 - Common cloud models 4.1.1.1 - Private cloud 4.1.1.2 - Public cloud 4.1.1.3 - Hybrid cloud 4.1.1.4 - Community cloud 4.1.1.5 - Infrastructure as a service (IaaS) 4.1.1.6 - Software as a service (SaaS) 4.1.1.7 - Platform as a service (PaaS) 4.1.2 - Cloud characteristics 4.1.2.1 - Shared resources 4.1.2.2 - Metered utilization

		4.1.2.3 - Rapid elasticity 4.1.2.4 - High availability 4.1.2.5 - File synchronization
6.4	Virtualization	4.1 - Summarize cloud-computing concepts. 4.1.3 - Desktop virtualization 4.1.3.1 - Virtual desktop infrastructure (VDI) on premises 4.1.3.2 - VDI in the cloud 4.2 - Summarize aspects of client-side virtualization. 4.2.1 - Purpose of virtual machines 4.2.1.1 - Sandbox 4.2.1.2 - Test development 4.2.1.3 - Application virtualization 4.2.1.3.1 - Legacy software/OS 4.2.1.3.2 - Cross-platform virtualization 4.2.2 - Resource requirements
7.0	**System Management 1**	
7.1	Windows System Tools	
7.2	Windows Settings	
7.3	Performance Monitoring	

7.4	Windows Application Management	
7.5	Linux Application Management	
7.6	Digital Content Management	
7.7	Virtual Memory	3.2 - Given a scenario, install the appropriate RAM. 3.2.1 - RAM types 3.2.1.1 - Virtual RAM
7.8	Windows and Application Troubleshooting	
7.9	Scripting Basics	
8.0	**System Management 2**	
8.1	Active Directory	
8.2	Users and Groups	
8.3	Remote Services	
8.4	VPN	

8.5	Updates	
8.6	System Backup	
8.7	System Recovery	
8.8	Windows Boot Errors	
9.0	**File Management**	
9.1	Manage Files on Windows	
9.2	NTFS and Share Permissions	
9.3	File Encryption	3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards. 3.4.5 - Encryption 3.4.5.1 - TPM
9.4	Linux File Management	
10.0	**Peripheral Devices**	
10.1	Peripheral Devices	1.1 - Given a scenario, install and configure laptop hardware and components. 1.1.2 - Physical privacy and security components 1.1.2.1 - Biometrics

		1.1.2.2 - Near-field scanner features **1.2 - Compare and contrast the display components of mobile devices.** 1.2.5 - Microphone 1.2.6 - Touch screen/digitizer
10.2	Display Devices	**1.2 - Compare and contrast the display components of mobile devices.** 1.2.1 - Types 1.2.1.1 - Liquid crystal display (LCD) 1.2.1.2 - Organic light-emitting diode (OLED) 1.2.2 - Mobile display components
10.3	Display, Video, and Projector Troubleshooting	**5.4 - Given a scenario, troubleshoot video, projector, and display issues.** 5.4.1 - Common symptoms 5.4.1.1 - Incorrect data source 5.4.1.2 - Physical cabling issues 5.4.1.3 - Burned-out bulb 5.4.1.4 - Fuzzy image 5.4.1.5 - Display burn-in 5.4.1.6 - Dead pixels 5.4.1.7 - Flashing screen 5.4.1.8 - Incorrect color display 5.4.1.9 - Audio issues 5.4.1.10 - Dim image 5.4.1.11 - Intermittent projector shutdown

10.4	Device Driver Management	3.3 - Given a scenario, select and install storage devices.
		3.3.1 - Hard drives 3.3.4 - Removable storage
		3.4 - Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
		3.4.7 - Expansion cards
10.5	Device Driver Troubleshooting	5.3 - Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.
		5.3.1 - Common symptoms
11.0	**Networking**	
11.1	Networking Overview	2.1 - Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
		2.1.1 - Ports and protocols
		2.2 - Compare and contrast common networking hardware.
		2.2.11 - Network interface card (NIC)
		2.5 - Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
		2.5.1 - Internet Protocol (IP) adressing
		2.5.1.1 - IPv4

		2.7 - Compare and contrast Internet connection types, network types, and their features.
		
		2.7.2 - Network types
		
		    2.7.2.1 - Local area network (LAN)
		    2.7.2.2 - Wider area network (WAN)
		    2.7.2.3 - Personal area network (PAN)
		    2.7.2.4 - Metropolitan area network (MAN)
		    2.7.2.5 - Storage area network (SAN)
		    2.7.2.6 - Wireless local area network (WLAN)

11.2	Networking Ports and Protocols	2.1 - Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
		
		2.1.1 - Ports and protocols
		
		    2.1.1.1 - 20/21--File Transfer Protocol (FTP)
		    2.1.1.2 - 22--Secure Shell (SSH)
		    2.1.1.3 - 23--Telnet
		    2.1.1.4 - 25--Simple Mail Transfer Protocol (SMTP)
		    2.1.1.5 - 53--Domain Name System (DNS)
		    2.1.1.6 - 67/68--Dynamic Host Configuration Protocol (DHCP)
		    2.1.1.7 - 80--Hypertext Transfer Protocol (HTTP)
		    2.1.1.8 - 110--Post Office Protocol 3 (POP3)
		    2.1.1.9 - 137/139--Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)
		    2.1.1.10 - 143--Internet Mail Access Protocol (IMAP)
		    2.1.1.11 - 161/162--Simple Network Management Protocol (SNMP)
		    2.1.1.12 - 389--Lightweight Directory Access Protocol (LDAP)
		    2.1.1.13 - 443--Hypertext Transfer Protocol Secure (HTTPS)
		    2.1.1.14 - 445--Server Message Block (SMB)/Common Internet File System (CFIS)
		    2.1.1.15 - 3389--Remote Desktop Protocol (RDP)
		
		2.1.2 - TCP vs. UDP

		2.1.2.1 - Connectionless
		    o 2.1.2.1.1 - DHCP
		    o 2.1.2.1.2 - Trivial File Transfer Protocol (TFTP)
		2.1.2.2 - Connection-oriented
		    o 2.1.2.2.1 - HTTPS
		    o 2.1.2.2.2 - SSH

11.3	Client-Side Network Configuration	**2.5 - Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.**
		
		2.5.1 - Internet Protocol (IP) addressing
		
		2.5.1.1 - IPv4
		    o 2.5.1.1.1 - Private addresses
		    o 2.5.1.1.2 - Public addresses
		2.5.1.2 - IPv6
		2.5.1.3 - Automatic Private IP Addressing (APIPA)
		2.5.1.4 - Static
		2.5.1.5 - Dynamic
		2.5.1.6 - Gateway
		
		2.6 - Compare and contrast common network configuration concepts.
		
		2.6.1 - DNS
		2.6.2 - DHCP

11.4	Services Provided by Network Devices	**2.4 - Summarize services provided by networked hosts.** 2.4.1 - Server roles 2.4.1.1 - DNS 2.4.1.2 - DHCP 2.4.1.3 - Fileshare 2.4.1.4 - Print servers 2.4.1.5 - Mail servers

2.4.1.6 - Syslog
2.4.1.7 - Web servers
2.4.1.8 - Authentication, authorization, and accounting (AAA)

2.4.2 - Internet appliances

2.4.2.1 - Spam gateways
2.4.2.2 - Unified threat management (UTM)
2.4.2.3 - Load balancers
2.4.2.4 - Proxy servers

2.4.3 - Legacy/embedded systems

2.4.3.1 - Supervisory control and data acquisition (SCADA)

2.4.4 - Internet of Things (IoT) devices

2.6 - Compare and contrast common network configuration concepts.

2.6.1 - DNS

2.6.1.1 - Address
  o   2.6.1.1.1 - A
  o   2.6.1.1.2 - AAAA
2.6.1.2 - Mail exchanger (MX)
2.6.1.3 - Text (TXT)
  o   2.6.1.3.1 - Spam management
       ▪   2.6.1.3.1.1 - DomainKeys Identified Mail (DKIM)
       ▪   2.6.1.3.1.2 - Sender Policy Framework (SPF)
       ▪   2.6.1.3.1.3 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)

		2.6.2 - DHCP 2.6.2.1 - Leases 2.6.2.2 - Reservations 2.6.2.3 - Scope
11.5	Wireless Networking	1.4 - Given a scenario, configure basic mobile-device network connectivity and application support. 1.4.2 - Bluetooth 1.4.2.1 - Enable Bluetooth 1.4.2.2 - Enable pairing 1.4.2.3 - Find a device for pairing 1.4.2.4 - Enter the appropriate PIN code 1.4.2.5 - Test connectivity 2.3 - Compare and contrast protocols for wireless networking. 2.3.1 - Frequencies 2.3.1.1 - 2.4GHz 2.3.1.2 - 5GHz 2.3.2 - Channels 2.3.2.1 - Regulations 2.3.2.2 - 2.4GHz vs. 5GHz 2.3.3 - Bluetooth 2.3.4 - 802.11 2.3.4.1 - a 2.3.4.2 - b 2.3.4.3 - g 2.3.4.4 - n

		2.3.4.5 - ac (WiFi 5) 2.3.4.6 - ax (WiFi 6) 2.3.5 - Long-range fixed wireless 2.3.5.1 - Licensed 2.3.5.2 - Unlicensed 2.3.5.3 - Power 2.3.5.4 - Regulatory requirements for wireless power 2.3.6 - NFC 2.3.7 - Radio-frequency identification (RFID)
11.6	SOHO Configuration	
11.7	Networking Hardware	2.2 - Compare and contrast common networking hardware. 2.2.1 - Routers 2.2.2 - Switches 2.2.2.1 - Managed 2.2.2.2 - Unmanaged 2.2.3 - Access points 2.2.4 - Patch panel 2.2.5 - Firewall 2.2.6 - Power over Ethernet (PoE) 2.2.6.1 - Injectors 2.2.6.2 - Switch 2.2.6.3 - PoE standards 2.2.7 - Hub 2.2.12 - Software-defined networking (SDN)

		2.6 - Compare and contrast common network configuration concepts.
		
		    2.6.3 - Virtual LAN (VLAN)
		    2.6.4 - Virtual private network (VPN)
		
		2.7 - Compare and contrast Internet connection types, network types, and their features.
		
		    2.7.1 - Internet connection types
		
		        2.7.1.1 - Satellite
		        2.7.1.2 - Fiber
		        2.7.1.3 - Cable
		        2.7.1.4 - DSL
		        2.7.1.5 - Cellular
		        2.7.1.6 - Wireless Internet service provider (WISP)

11.8	Command Line Network Utilities	

11.9	Network Troubleshooting	2.5 - Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.
		
		    2.5.1 - Internet Protocol (IP) adressing
		
		        2.5.1.1 - IPv4
		        2.5.1.4 - Static
		
		5.7 - Given a scenario, troubleshoot problems with wired and wireless networks.
		
		    5.7.1 - Common symptoms
		
		        5.7.1.1 - Intermittent wireless connectivity
		        5.7.1.2 - Slow network speeds
		        5.7.1.3 - Limited connectivity

		5.7.1.4 - Jitter 5.7.1.5 - Poor Voice over Internet Protocol (VoIP) quality 5.7.1.6 - Port flapping 5.7.1.7 - High latency 5.7.1.8 - External interference
12.0	**Mobile Devices**	
12.1	Laptops	1.1 - Given a scenario, install and configure laptop hardware and components. 1.1.1 - Hardware/device replacement 1.1.1.1 - Battery 1.1.1.2 - Keyboard/keys 1.1.1.3 - Random-access memory (RAM) 1.1.1.4 - Hard disk drive (HDD)/solid-state drive (SSD) migration 1.1.1.5 - HDD/SSD replacement 1.1.1.6 - Wireless cards 1.2 - Compare and contrast the display components of mobile devices. 1.2.1 - Types 1.2.1.1 - Liquid crystal display (LCD) 1.3 - Given a scenario, set up and configure accessories and ports of mobile devices. 1.3.1 - Connection methods 1.3.1.1 - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB 1.3.1.3 - Serial interfaces 1.3.1.5 - Bluetooth

		1.3.2 - Accessories 1.3.2.4 - Webcam 1.3.3 - Docking station 1.3.4 - Port replicator 1.3.5 - Trackpad/drawing pad

12.2	Mobile Device Displays and Components	1.2 - Compare and contrast the display components of mobile devices.
		
		   1.2.1 - Types
		
		      1.2.1.1 - Liquid crystal display (LCD)
		         o 1.2.1.1.1 - In-plane switching (IPS)
		         o 1.2.1.1.2 - Twisted nematic (TN)
		         o 1.2.1.1.3 - Vertical alignment (VA)
		      1.2.1.2 - Organic light-emitting diode (OLED)
		
		   1.2.2 - Mobile display components
		   1.2.3 - WiFi antenna connector/placement
		   1.2.4 - Camera/webcam
		   1.2.5 - Microphone
		   1.2.6 - Touch screen/digitizer
		   1.2.7 - Inverter

12.3	Laptop Power Management	1.1 - Given a scenario, install and configure laptop hardware and components.
		
		   1.1.1 - Hardware/device replacement
		
		      1.1.1.1 - Battery

12.4	Mobile Devices	1.2 - Compare and contrast the display components of mobile devices.

		1.2.1 - Types
		
		    1.2.1.1 - Liquid crystal display (LCD)
		
		1.2.2 - Mobile display components
		1.2.4 - Camera/webcam
		1.2.5 - Microphone
		1.2.6 - Touch screen/digitizer
		
		1.3 - Given a scenario, set up and configure accessories and ports of mobile devices.
		
		1.3.1 - Connection methods
		
		    1.3.1.1 - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB
		    1.3.1.2 - Lightning
		    1.3.1.3 - Serial interfaces
		    1.3.1.4 - Near-field communication (NFC)
		    1.3.1.5 - Bluetooth
		    1.3.1.6 - Hotspot
		
		1.3.2 - Accessories
		
		    1.3.2.1 - Touch pens
		    1.3.2.2 - Headsets
		    1.3.2.3 - Speakers
		    1.3.2.4 - Webcam
		
		1.3.3 - Docking station
		1.3.4 - Port replicator
		1.3.5 - Trackpad/drawing pad

12.5	Mobile Device Network Connectivity	**1.3 - Given a scenario, set up and configure accessories and ports of mobile devices.** 1.3.1 - Connection methods

| | | 1.3.1.1 - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB
1.3.1.2 - Lightning
1.3.1.4 - Near-field communication (NFC)
1.3.1.5 - Bluetooth
1.3.1.6 - Hotspot

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

    1.4.1 - Wireless/cellular data network (enable/disable)

        1.4.1.1 - 2G/3G/4G/5G
        1.4.1.2 - Hotspot
        1.4.1.3 - Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)
        1.4.1.4 - Preferred Roaming List (PRL) updates

    1.4.2 - Bluetooth

        1.4.2.1 - Enable Bluetooth

    1.4.3 - Location services

        1.4.3.1 - Global Positioning System (GPS) services
        1.4.3.2 - Cellular location services

    1.4.4 - Mobile device management (MDM)/mobile application management (MAM)

        1.4.4.1 - Corporate email configuration
        1.4.4.2 - Two-factor authentication
        1.4.4.3 - Corporate applications

    1.4.5 - Mobile device synchronization

        1.4.5.1 - Recognizing data caps
        1.4.5.2 - Microsoft 365
        1.4.5.3 - ActiveSync |

		1.4.5.4 - Calendar
		1.4.5.5 - Contacts
		1.4.5.6 - Commercial mail application
		
		2.6 - Compare and contrast common network configuration concepts.
		
		    2.6.4 - Virtual private network (VPN)
		
		3.1 - Explain basic cable types and their connectors, features, and purposes.
		
		    3.1.6 - Connector types
		
		        3.1.6.12 - Lightning port

12.6	Mobile Device Security	1.1 - Given a scenario, install and configure laptop hardware and components.
		
		    1.1.2 - Physical privacy and security components
		
		        1.1.2.1 - Biometrics
		        1.1.2.2 - Near-field scanner features
		
		1.4 - Given a scenario, configure basic mobile-device network connectivity and application support.
		
		    1.4.1 - Wireless/cellular data network (enable/disable)
		    1.4.4 - Mobile device management (MDM)/mobile application management (MAM)

12.7	Laptop and Mobile Device Troubleshooting	1.1 - Given a scenario, install and configure laptop hardware and components.
		
		    1.1.1 - Hardware/device replacement
		
		        1.1.1.1 - Battery

		5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.
		5.2.1 - Common symptoms
		5.2.1.3 - Black screen
		5.5 - Given a scenario, troubleshoot common issues with mobile devices.
		5.5.1 - Common symptoms
		5.5.1.1 - Poor battery health 5.5.1.2 - Swollen battery 5.5.1.3 - Broken screen 5.5.1.4 - Improper charging 5.5.1.5 - Poor/no connectivity 5.5.1.6 - Liquid damage 5.5.1.7 - Overheating 5.5.1.8 - Digitizer issues 5.5.1.9 - Physically damaged ports 5.5.1.10 - Malware 5.5.1.11 - Cursor drift/touch calibration
		5.7 - Given a scenario, troubleshoot problems with wired and wireless networks.
		5.7.1 - Common symptoms
		5.7.1.1 - Intermittent wireless connectivity
13.0	**Printing**	
13.1	Printer Overview	3.6 - Given a scenario, deploy and configure multifunction devices/printers and settings.
		3.6.1 - Properly unboxing a device--set up location considerations

		3.6.2 - Use appropriate drivers for a given OS
		3.6.2.1 - Printer Control Language (PCL) vs. PostScript
		3.6.4 - Public/shared devices
		3.6.4.1 - Printer share
		3.6.5 - Configuration settings 3.6.6 - Security
		5.6 - Given a scenario, troubleshoot and resolve printer issues.
		5.6.1 - Common symptoms
		5.6.1.9 - Multiple prints pending in queue
13.2	Print Connectivity	**1.4 - Given a scenario, configure basic mobile-device network connectivity and application support.**
		1.4.2 - Bluetooth
		3.6 - Given a scenario, deploy and configure multifunction devices/printers and settings.
		3.6.2 - Use appropriate drivers for a given OS 3.6.3 - Device connectivity
		3.6.3.1 - USB 3.6.3.2 - Ethernet 3.6.3.3 - Wireless
		3.6.4 - Public/shared devices
		3.6.4.1 - Printer share

3.6.4.2 - Print server

3.6.6 - Security

3.6.6.4 - Secured prints

3.6.7 - Network scan services

3.6.7.1 - Email
3.6.7.2 - SMB
3.6.7.3 - Cloud services

3.6.8 - Automatic document feeder (ADF)/flatbed scanner

4.1 - Summarize cloud-computing concepts.

4.1.1 - Common cloud models

4.1.1.2 - Public cloud
4.1.1.4 - Community cloud

4.1.2 - Cloud characteristics

4.1.2.1 - Shared resources
4.1.2.5 - File synchronization

5.6 - Given a scenario, troubleshoot and resolve printer issues.

5.6.1 - Common symptoms

5.6.1.9 - Multiple prints pending in queue

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

		5.7.1 - Common symptoms
		5.7.1.3 - Limited connectivity
13.3	Printer Types and Components	3.6 - Given a scenario, deploy and configure multifunction devices/printers and settings.
		3.6.5 - Configuration settings
		3.6.5.1 - Duplex
		3.7 - Given a scenario, install and replace printer consumables.
		3.7.1 - Laser
		3.7.1.1 Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, duplexing assembly 3.7.1.2 Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning 3.7.1.3 Maintenance: Replace toner, apply maintenance kit, calibrate, clean
		3.7.2 - Inkjet
		3.7.2.1 Ink cartridge, print head, roller, feeder, duplexing assembly, carriage belt 3.7.2.2 Calibration 3.7.2.3 Maintenance: Clean heads, replace cartridges, calibrate, clear jams
		3.7.3 - Thermal
		3.7.3.1 - Feed assembly, heating element 3.7.3.2 - Special thermal paper 3.7.3.3 - Maintenance: Replace paper, clean heating element, remove debris

		3.7.3.4 - Heat sensitivity of paper
		
		3.7.4 - Impact
		
		    3.7.4.1 - Print head, ribbon, tractor feed
		    3.7.4.2 - Impact paper
		    3.7.4.3 - Maintenance: Replace ribbon, replace print head, replace paper
		
		3.7.5 - 3-D printer
		
		    3.7.5.1 - Filament
		    3.7.5.2 - Resin
		    3.7.5.3 - Print bed
		
		5.6 - Given a scenario, troubleshoot and resolve printer issues.
		
		    5.6.1 - Common symptoms
		
		        5.6.1.4 - Paper jams
		        5.6.1.5 - Faded print
		        5.6.1.10 - Speckling on printed pages
		        5.6.1.11 - Double/echo images on the print

13.4	Printer Troubleshooting	3.6 - Given a scenario, deploy and configure multifunction devices/printers and settings.
		
		    3.6.2 - Use appropriate drivers for a given OS
		
		3.7 - Given a scenario, install and replace printer consumables.
		
		    3.7.1 - Laser
		
		5.6 - Given a scenario, troubleshoot and resolve printer issues.

		5.6.1 - Common symptoms
		
		    5.6.1.1 - Lines down the printed pages
		    5.6.1.2 - Garbled print
		    5.6.1.3 - Toner not fusing to paper
		    5.6.1.4 - Paper jams
		    5.6.1.5 - Faded print
		    5.6.1.6 - Incorrect paper size
		    5.6.1.7 - Paper not feeding
		    5.6.1.8 - Multipage misfeed
		    5.6.1.9 - Multiple prints pending in queue
		    5.6.1.10 - Speckling on printed pages
		    5.6.1.11 - Double/echo images on the print
		    5.6.1.12 - Incorrect chroma display
		    5.6.1.13 - Grinding noise
		    5.6.1.14 - Finishing issues
		    5.6.1.14.1 - Staple jams
		    5.6.1.14.2 - Hole punch
		    5.6.1.15 - Incorrect page orientation

14.0	**Security**	
14.1	Security Best Practices	
14.2	Incident Response and Regulated Data	
14.3	Physical Security	
14.4	Logical Security Measures	
14.5	Social Engineering Attacks	

14.6	Data Destruction and Disposal	
14.7	Malware Protection	
14.8	Firewalls	2.2 - Compare and contrast common networking hardware. 2.2.5 - Firewall 2.4 - Summarize services provided by networked hosts. 2.4.2 - Internet appliances 2.4.2.2 - Unified threat management (UTM)
14.9	Proxy Servers	2.4 - Summarize services provided by networked hosts. 2.4.2 - Internet appliances 2.4.2.4 - Proxy servers
14.10	Install, Configure, and Secure Browsers	
14.11	Security Troubleshooting	
15.0	**Capstone Exercises**	
		1.3 - Given a scenario, set up and configure accessories and ports of mobile devices. 1.3.1 - Connection methods

1.3.1.5 - Bluetooth

3.2 - Given a scenario, install the appropriate RAM.

3.2.3 - Dual-channel

3.3 - Given a scenario, select and install storage devices.

3.3.3 - Drive configurations

3.3.3.1 - Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10

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

3.4.2 - Motherboard connector types

3.4.2.3 - Power connectors
3.4.2.4 - SATA

3.4.4 - Basic Input/Output System (BIOS)/Unified Extemsible Firmware Interface (UEFI) settings
3.4.7 - Expansion cards
3.4.8 - Cooling

3.4.8.1 - Fans
3.4.8.2 - Heat sink

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

3.5.5 - Modular power supply

		5.2 - Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.
		5.2.1 - Common symptoms
		5.3 - Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.
		5.3.1 - Common symptoms
		5.3.1.6 - RAID failure
		5.7 - Given a scenario, troubleshoot problems with wired and wireless networks.
		5.7.1 - Common symptoms
A.0	**TestOut PC Pro - Practice Exams**	
A.1	Prepare for TestOut PC Pro Certification	
A.2	TestOut PC Pro Exam Domain Review	
A.3	TestOut PC Pro Certification Practice Exam	
B.0	**CompTIA A+ Core 1 (220-1101) - Practice Exams**	

B.1	Prepare for CompTIA A+ Core 1 (220-1101) Certification	
B.2	CompTIA A+ Core 1 (220-1101) Domain Review (20 Questions)	
B.3	CompTIA A+ Core 1 (220-1101) Domain Review (All Questions)	
C.0	**CompTIA A+ Core 2 (220-1102) - Practice Exams**	
C.1	Prepare for CompTIA A+ Core 2 (220-1102) Certification	
C.2	CompTIA A+ Core 2 (220-1102) Domain Review (20 Questions)	
C.3	CompTIA A+ Core 2 (220-1102) Domain Review (All Questions)	

Objective Mapping: CompTIA 220-1101 Objectives to LabSim Section

The TestOut PC Pro course and certification exam cover the following CompTIA A+ Certification 220-1101 objectives:

#	Domain	Module.Section
1.0	**Mobile Devices**	
1.1	Given a scenario, install and configure laptop hardware and components. 1.1.1 - Hardware/device replacement o 1.1.1.1 - Battery o 1.1.1.2 - Keyboard/keys o 1.1.1.3 - Random-access memory (RAM) o 1.1.1.4 - Hard disk drive (HDD)/solid-state drive (SSD) migration o 1.1.1.5 - HDD/SSD replacement o 1.1.1.6 - Wireless cards 1.1.2 - Physical privacy and security components o 1.1.2.1 - Biometrics o 1.1.2.2 - Near-field scanner features	1.1 2.5 5.8 10.1 12.1, 12.3, 12.6, 12.7
1.2	Compare and contrast the display components of mobile devices. 1.2.1 - Types o 1.2.1.1 - Liquid crystal display (LCD) o 1.2.1.1.1 - In-plane switching (IPS) o 1.2.1.1.2 - Twisted nematic (TN) o 1.2.1.1.3 - Vertical alignment (VA) o 1.2.1.2 - Organic light-emitting diode (OLED) 1.2.2 - Mobile display components 1.2.3 - WiFi antenna connector/placement 1.2.4 - Camera/webcam 1.2.5 - Microphone 1.2.6 - Touch screen/digitizer 1.2.7 - Inverter	10.1, 10.2 12.1, 12.2, 12.4
1.3	Given a scenario, set up and configure accessories and ports of mobile devices.	12.1, 12.4, 12.5

		1.3.1 - Connection methods
		    o 1.3.1.1 - Universal Serial Bus (USB)/USB-C/microUSB/miniUSB
		    o 1.3.1.2 - Lightning
		    o 1.3.1.3 - Serial interfaces
		    o 1.3.1.4 - Near-field communication (NFC)
		    o 1.3.1.5 - Bluetooth
		    o 1.3.1.6 - Hotspot
		1.3.2 - Accessories
		    o 1.3.2.1 - Touch pens
		    o 1.3.2.2 - Headsets
		    o 1.3.2.3 - Speakers
		    o 1.3.2.4 - Webcam
		1.3.3 - Docking station
		1.3.4 - Port replicator
		1.3.5 - Trackpad/drawing pad
			14.11

1.4		Given a scenario, configure basic mobile-device network connectivity and application support.
		
		1.4.1 - Wireless/cellular data network (enable/disable)
		    o 1.4.1.1 - 2G/3G/4G/5G
		    o 1.4.1.2 - Hotspot
		    o 1.4.1.3 - Global System for Mobile Communications (GSM) vs. code-division multiple access (CDMA)
		    o 1.4.1.4 - Preferred Roaming List (PRL) updates
		1.4.2 - Bluetooth
		    o 1.4.2.1 - Enable Bluetooth
		    o 1.4.2.2 - Enable pairing
		    o 1.4.2.3 - Find a device for pairing
		    o 1.4.2.4 - Enter the appropriate PIN code
		    o 1.4.2.5 - Test connectivity
		1.4.3 - Location services
		    o 1.4.3.1 - Global Positioning System (GPS) services
		    o 1.4.3.2 - Cellular location services
		1.4.4 - Mobile device management (MDM)/mobile application management (MAM)
		    o 1.4.4.1 - Corporate email configuration
		    o 1.4.4.2 - Two-factor authentication
			11.5
			12.5, 12.6
			
			13.2

	o 1.4.4.3 - Corporate applications
	1.4.5 - Mobile device synchronization
	    o 1.4.5.1 - Recognizing data caps
	    o 1.4.5.2 - Microsoft 365
	    o 1.4.5.3 - ActiveSync
	    o 1.4.5.4 - Calendar
	    o 1.4.5.5 - Contacts
	    o 1.4.5.6 - Commercial mail application	

2.0	**Networking**	

2.1	Compare and contrast Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports, protocols, and their purposes.
	
	2.1.1 - Ports and protocols
	    o 2.1.1.1 - 20/21--File Transfer Protocol (FTP)
	    o 2.1.1.2 - 22--Secure Shell (SSH)
	    o 2.1.1.3 - 23--Telnet
	    o 2.1.1.4 - 25--Simple Mail Transfer Protocol (SMTP)
	    o 2.1.1.5 - 53--Domain Name System (DNS)
	    o 2.1.1.6 - 67/68--Dynamic Host Configuration Protocol (DHCP)
	    o 2.1.1.7 - 80--Hypertext Transfer Protocol (HTTP)
	    o 2.1.1.8 - 110--Post Office Protocol 3 (POP3)
	    o 2.1.1.9 - 137/139--Network Basic Input/Output System (NetBIOS)/NetBIOS over TCP/IP (NetBT)
	    o 2.1.1.10 - 143--Internet Mail Access Protocol (IMAP)
	    o 2.1.1.11 - 161/162--Simple Network Management Protocol (SNMP)
	    o 2.1.1.12 - 389--Lightweight Directory Access Protocol (LDAP)
	    o 2.1.1.13 - 443--Hypertext Transfer Protocol Secure (HTTPS)
	    o 2.1.1.14 - 445--Server Message Block (SMB)/Common Internet File System (CFIS)
	    o 2.1.1.15 - 3389--Remote Desktop Protocol (RDP)
	2.1.2 - TCP vs. UDP
	    o 2.1.2.1 - Connectionless
	    o 2.1.2.1.1 - DHCP
	    o 2.1.2.1.2 - Trivial File Transfer Protocol (TFTP)
		11.1, 11.2

	o 2.1.2.2 - Connection-oriented o 2.1.2.2.1 - HTTPS o 2.1.2.2.2 - SSH	

2.2	Compare and contrast common networking hardware.
	
	2.2.1 - Routers
	2.2.2 - Switches
	    o 2.2.2.1 - Managed
	    o 2.2.2.2 - Unmanaged
	2.2.3 - Access points
	2.2.4 - Patch panel
	2.2.5 - Firewall
	2.2.6 - Power over Ethernet (PoE)
	    o 2.2.6.1 - Injectors
	    o 2.2.6.2 - Switch
	    o 2.2.6.3 - PoE standards
	2.2.7 - Hub
	2.2.8 - Cable modem
	2.2.9 - Digital subscriber line (DSL)
	2.2.10 - Optical network terminal (ONT)
	2.2.11 - Network interface card (NIC)
	2.2.12 - Software-defined networking (SDN)
		1.1
		11.1, 11.7
		
		14.8

2.3	Compare and contrast protocols for wireless networking.
	
	2.3.1 - Frequencies
	    o 2.3.1.1 - 2.4GHz
	    o 2.3.1.2 - 5GHz
	2.3.2 - Channels
	    o 2.3.2.1 - Regulations
	    o 2.3.2.2 - 2.4GHz vs. 5GHz
	2.3.3 - Bluetooth
	2.3.4 - 802.11
	    o 2.3.4.1 - a
		11.5

		o 2.3.4.2 - b
		o 2.3.4.3 - g
		o 2.3.4.4 - n
		o 2.3.4.5 - ac (WiFi 5)
		o 2.3.4.6 - ax (WiFi 6)
		2.3.5 - Long-range fixed wireless
		     o 2.3.5.1 - Licensed
		     o 2.3.5.2 - Unlicensed
		     o 2.3.5.3 - Power
		     o 2.3.5.4 - Regulatory requirements for wireless power
		2.3.6 - NFC
		2.3.7 - Radio-frequency identification (RFID)	

2.4	Summarize services provided by networked hosts.
	
	2.4.1 - Server roles
	     o 2.4.1.1 - DNS
	     o 2.4.1.2 - DHCP
	     o 2.4.1.3 - Fileshare
	     o 2.4.1.4 - Print servers
	     o 2.4.1.5 - Mail servers
	     o 2.4.1.6 - Syslog
	     o 2.4.1.7 - Web servers
	     o 2.4.1.8 - Authentication, authorization, and accounting (AAA)
	2.4.2 - Internet appliances
	     o 2.4.2.1 - Spam gateways
	     o 2.4.2.2 - Unified threat management (UTM)
	     o 2.4.2.3 - Load balancers
	     o 2.4.2.4 - Proxy servers
	2.4.3 - Legacy/embedded systems
	     o 2.4.3.1 - Supervisory control and data acquisition (SCADA)
	2.4.4 - Internet of Things (IoT) devices
		11.4
		14.8, 14.9	

2.5	Given a scenario, install and configure basic wired/wireless small office/home office (SOHO) networks.	11.1, 11.3, 11.9	

	2.5.1 - Internet Protocol (IP) adressing
	     o 2.5.1.1 - IPv4
	     o 2.5.1.1.1 - Private addresses
	     o 2.5.1.1.2 - Public addresses
	     o 2.5.1.2 - IPv6
	     o 2.5.1.3 - Automatic Private IP Addressing (APIPA)
	     o 2.5.1.4 - Static
	     o 2.5.1.5 - Dynamic
	     o 2.5.1.6 - Gateway		

2.6	Compare and contrast common network configuration concepts.
	
	    2.6.1 - DNS
	          o 2.6.1.1 - Address
	          o 2.6.1.1.1 - A
	          o 2.6.1.1.2 - AAAA
	          o 2.6.1.2 - Mail exchanger (MX)
	          o 2.6.1.3 - Text (TXT)
	          o 2.6.1.3.1 - Spam management
	          o 2.6.1.3.1.1 - DomainKeys Identified Mail (DKIM)
	          o 2.6.1.3.1.2 - Sender Policy Framework (SPF)
	          o 2.6.1.3.1.3 - Domain-based Message Authentication, Reporting, and Conformance (DMARC)
	    2.6.2 - DHCP
	          o 2.6.2.1 - Leases
	          o 2.6.2.2 - Reservations
	          o 2.6.2.3 - Scope
	    2.6.3 - Virtual LAN (VLAN)
	    2.6.4 - Virtual private network (VPN)
			11.3, 11.4, 11.7
			12.5

2.7	Compare and contrast Internet connection types, network types, and their features.
	
	    2.7.1 - Internet connection types
	          o 2.7.1.1 - Satellite
	          o 2.7.1.2 - Fiber
			11.1, 11.7

	o 2.7.1.3 - Cable
	     o 2.7.1.4 - DSL
	     o 2.7.1.5 - Cellular
	     o 2.7.1.6 - Wireless Internet service provider (WISP)
	  2.7.2 - Network types
	     o 2.7.2.1 - Local area network (LAN)
	     o 2.7.2.2 - Wider area network (WAN)
	     o 2.7.2.3 - Personal area network (PAN)
	     o 2.7.2.4 - Metropolitan area network (MAN)
	     o 2.7.2.5 - Storage area network (SAN)
	     o 2.7.2.6 - Wireless local area network (WLAN)	

2.8	Given a scenario, use networking tools.
	
	  2.8.1 - Crimper
	  2.8.2 - Cable stripper
	  2.8.3 - WiFi analyzer
	  2.8.4 - Toner probe
	  2.8.5 - Punchdown tool
	  2.8.6 - Cable tester
	  2.8.7 - Loopback plug
	  2.8.8 - Network tap
		2.6

3.0	**Hardware**	

3.1	Explain basic cable types and their connectors, features, and purposes.
	
	  3.1.1 - Network cables
	     o 3.1.1.1 - Copper
	     o 3.1.1.1.1 - Cat 5
	     o 3.1.1.1.2 - Cat 5e
	     o 3.1.1.1.3 - Cat 6
	     o 3.1.1.1.4 - Cat 6a
	     o 3.1.1.1.5 - Coaxial
	     o 3.1.1.1.6 - Shielded twisted pair
		3.1, 3.2, 3.11
		5.2
		
		12.5

   o 3.1.1.1.6.1 - Direct burial
   o 3.1.1.1.7 - Unshielded twisted pair
   o 3.1.1.2 - Plenum
   o 3.1.1.3 - Optical
   o 3.1.1.3.1 - Fiber
   o 3.1.1.4 - T568A/T568B
  3.1.2 - Peripheral cables
   o 3.1.2.1 - USB 2.0
   o 3.1.2.2 - USB 3.0
   o 3.1.2.3 - Serial
   o 3.1.2.4 - Thunderbolt
  3.1.3 - Video cables
   o 3.1.3.1 - High-Definition Multimedia Interface (HDMI)
   o 3.1.3.2 - DisplayPort
   o 3.1.3.3 - Digital Visual Interface (DVI)
   o 3.1.3.4 - Video Graphics Array (VGA)
  3.1.4 - Hard drive cables
   o 3.1.4.1 - Serial Advanced Technology Attachment (SATA)
   o 3.1.4.2 - Small Computer System Interface (SCSI)
   o 3.1.4.3 - External SATA (eSATA)
   o 3.1.4.4 - Integrated Drive Electronics (IDE)
  3.1.5 - Adapters
  3.1.6 - Connector types
   o 3.1.6.1 - RJ11
   o 3.1.6.2 - RJ45
   o 3.1.6.3 - F type
   o 3.1.6.4 - Straight tip (ST)
   o 3.1.6.5 - Subscriber connector (SC)
   o 3.1.6.6 - Lucent connector (LC)
   o 3.1.6.7 - Punchdown block
   o 3.1.6.8 - microUSB
   o 3.1.6.9 - miniUSB
   o 3.1.6.10 - USB-C
   o 3.1.6.11 - Molex
   o 3.1.6.12 - Lightning port
   o 3.1.6.13 - DB9

3.2	Given a scenario, install the appropriate RAM.	3.5, 3.6
		7.7
	3.2.1 - RAM types	
	o 3.2.1.1 - Virtual RAM	14.11
	o 3.2.1.2 - Small outline dual inline memory module (SODIMM)	
	o 3.2.1.3 - Double Data Rate 3 (DDR3)	
	o 3.2.1.4 - Double Data Rate 4 (DDR4)	
	o 3.2.1.5 - Double Data Rate 5 (DDR5)	
	o 3.2.1.6 - Error correction code (ECC) RAM	
	3.2.2 - Single-channel	
	3.2.3 - Dual-channel	
	3.2.4 - Triple-channel	
	3.2.5 - Quad-channel	
3.3	Given a scenario, select and install storage devices.	1.1
		5.1, 5.2, 5.3, 5.4, 5.7, 5.8, 5.9
	3.3.1 - Hard drives	
	o 3.3.1.1 - Speeds	6.2
	o 3.3.1.1.1 - 5,400rpm	
	o 3.3.1.1.2 - 7,200rpm	10.4
	o 3.3.1.1.3 - 10,000rpm	
	o 3.3.1.1.4 - 15,000rpm	14.11
	o 3.3.1.2 - Form factor	
	o 3.3.1.2.1 - 2.5	
	o 3.3.1.2.2 - 3.5	
	3.3.2 - SSDs	
	o 3.3.2.1 - Communications interfaces	
	o 3.3.2.1.1 - Non-volatile Memory Express (NVMe)	
	o 3.3.2.1.2 - SATA	
	o 3.3.2.1.3 - Peripheral Component Interconnect Express (PCIe)	
	o 3.3.2.2 - Form Factors	
	o 3.3.2.2.1 - M2	
	o 3.3.2.2.2 - mSATA	
	3.3.3 - Drive configurations	
	o 3.3.3.1 - Redundant Array of Independent (or Inexpensive) Disks (RAID) 0, 1, 5, 10	

	3.3.4 - Removable storage
	    o 3.3.4.1 - Flash drives
	    o 3.3.4.2 - Memory cards
	    o 3.3.4.3 - Optical drives	

3.4	Given a scenario, install and configure motherboards, central processing units (CPUs), and add-on cards.
	
	3.4.1 - Motherboard form factor
	    o 3.4.1.1 - Advanced Technology eXtended (ATX)
	    o 3.4.1.2 - Information Technology eXtended (ITX)
	3.4.2 - Motherboard connector types
	    o 3.4.2.1 - Peripheral Component Interconnect (PCI)
	    o 3.4.2.2 - PCI Express (PCIe)
	    o 3.4.2.3 - Power connectors
	    o 3.4.2.4 - SATA
	    o 3.4.2.5 - eSATA
	    o 3.4.2.6 - SAN
	    o 3.4.2.7 - Headers
	    o 3.4.2.8 - M.2
	3.4.3 - Motherboard compatibility
	    o 3.4.3.1 - CPU sockets
	    o 3.4.3.1.1 - Advanced Micro Devices, Inc. (AMD)
	    o 3.4.3.1.2 - Intel
	    o 3.4.3.2 - Server
	    o 3.4.3.3 - Multisocket
	    o 3.4.3.4 - Desktop
	    o 3.4.3.5 - Mobile
	3.4.4 - Basic Input/Output System (BIOS)/Unified Extemsible Firmware Interface (UEFI) settings
	    o 3.4.4.1 - Boot options
	    o 3.4.4.2 - USB permissions
	    o 3.4.4.3 - Trusted Platform Module (TPM) security features
	    o 3.4.4.4 - Fan considerations
	    o 3.4.4.5 - Secure Boot
	    o 3.4.4.6 - Boot password
	3.4.5 - Encryption
	    o 3.4.5.1 - TPM
		2.5
		3.3, 3.8, 3.9, 3.10, 3.11, 3.12, 3.13, 3.14
		
		4.2
		
		5.2
		
		9.3
		
		10.4
		
		14.11

	o 3.4.5.2 - Hardware security module (HSM)
	3.4.6 - CPU architecture
	    o 3.4.6.1 - x64/x86
	    o 3.4.6.2 - Advanced RISC Machine (ARM)
	    o 3.4.6.3 - Single-core
	    o 3.4.6.4 - Multicore
	    o 3.4.6.5 - Multithreading
	    o 3.4.6.6 - Virtualization support
	3.4.7 - Expansion cards
	    o 3.4.7.1 - Sound card
	    o 3.4.7.2 - Video card
	    o 3.4.7.3 - Capture card
	    o 3.4.7.4 - NIC
	3.4.8 - Cooling
	    o 3.4.8.1 - Fans
	    o 3.4.8.2 - Heat sink
	    o 3.4.8.3 - Thermal paste/pads
	    o 3.4.8.4 - Liquid	

3.5	Given a scenario, install or replace the appropriate power supply.
	
	    3.5.1 - Input 115V vs. 220V
	    3.5.2 - Output 3.3V vs. 5V vs. 12V
	    3.5.3 - 20-pin to 24-pin motherboard adapter
	    3.5.4 - Redundant power supply
	    3.5.5 - Modular power supply
	    3.5.6 - Wattage rating
		3.14
		14.11

3.6	Given a scenario, deploy and configure multifunction devices/printers and settings.
	
	    3.6.1 - Properly unboxing a device--set up location considerations
	    3.6.2 - Use appropriate drivers for a given OS
	        o 3.6.2.1 - Printer Control Language (PCL) vs. PostScript
	    3.6.3 - Device connectivity
	        o 3.6.3.1 - USB
		3.2
		13.1, 13.2, 13.3, 13.4

	○ 3.6.3.2 - Ethernet
	○ 3.6.3.3 - Wireless
	3.6.4 - Public/shared devices
	   ○ 3.6.4.1 - Printer share
	   ○ 3.6.4.2 - Print server
	3.6.5 - Configuration settings
	   ○ 3.6.5.1 - Duplex
	   ○ 3.6.5.2 - Orientation
	   ○ 3.6.5.3 - Tray settings
	   ○ 3.6.5.4 - Quality
	3.6.6 - Security
	   ○ 3.6.6.1 - User authentication
	   ○ 3.6.6.2 - Badging
	   ○ 3.6.6.3 - Audit logs
	   ○ 3.6.6.4 - Secured prints
	3.6.7 - Network scan services
	   ○ 3.6.7.1 - Email
	   ○ 3.6.7.2 - SMB
	   ○ 3.6.7.3 - Cloud services
	3.6.8 - Automatic document feeder (ADF)/flatbed scanner	

3.7	Given a scenario, install and replace printer consumables.
	
	3.7.1 - Laser
	   ○ 3.7.1.1 Imaging drum, fuser assembly, transfer belt, transfer roller, pickup rollers, separation pads, duplexing assembly
	   ○ 3.7.1.2 Imaging process: processing, charging, exposing, developing, transferring, fusing, and cleaning
	   ○ 3.7.1.3 Maintenance: Replace toner, apply maintenance kit, calibrate, clean
	3.7.2 - Inkjet
	   ○ 3.7.2.1 Ink cartridge, print head, roller, feeder, duplexing assembly, carriage belt
	   ○ 3.7.2.2 Calibration
	   ○ 3.7.2.3 Maintenance: Clean heads, replace cartridges, calibrate, clear jams
	3.7.3 - Thermal
		2.5
		13.3, 13.4

	o 3.7.3.1 - Feed assembly, heating element
	o 3.7.3.2 - Special thermal paper
	o 3.7.3.3 - Maintenance: Replace paper, clean heating element, remove debris
	o 3.7.3.4 - Heat sensitivity of paper
	3.7.4 - Impact
	   o 3.7.4.1 - Print head, ribbon, tractor feed
	   o 3.7.4.2 - Impact paper
	   o 3.7.4.3 - Maintenance: Replace ribbon, replace print head, replace paper
	3.7.5 - 3-D printer
	   o 3.7.5.1 - Filament
	   o 3.7.5.2 - Resin
	   o 3.7.5.3 - Print bed	

4.0	**Virtualization and Cloud Computing**	

4.1	Summarize cloud-computing concepts.
	
	4.1.1 - Common cloud models
	   o 4.1.1.1 - Private cloud
	   o 4.1.1.2 - Public cloud
	   o 4.1.1.3 - Hybrid cloud
	   o 4.1.1.4 - Community cloud
	   o 4.1.1.5 - Infrastructure as a service (IaaS)
	   o 4.1.1.6 - Software as a service (SaaS)
	   o 4.1.1.7 - Platform as a service (PaaS)
	4.1.2 - Cloud characteristics
	   o 4.1.2.1 - Shared resources
	   o 4.1.2.2 - Metered utilization
	   o 4.1.2.3 - Rapid elasticity
	   o 4.1.2.4 - High availability
	   o 4.1.2.5 - File synchronization
	4.1.3 - Desktop virtualization
	   o 4.1.3.1 - Virtual desktop infrastructure (VDI) on premises
	   o 4.1.3.2 - VDI in the cloud
		6.3, 6.4
		13.2
		
		4.1

4.2	Summarize aspects of client-side virtualization.	6.4

4.2.1 - Purpose of virtual machines
- o 4.2.1.1 - Sandbox
- o 4.2.1.2 - Test development
- o 4.2.1.3 - Application virtualization
- o 4.2.1.3.1 - Legacy software/OS
- o 4.2.1.3.2 - Cross-platform virtualization

4.2.2 - Resource requirements
4.2.3 - Security requirements

5.0	**Hardware and Network Troubleshooting**	

5.1	Given a scenario, apply the best practice methodology to resolve problems.	2.7

5.1.1 - Always consider corporate policies, procedures, and impacts before implementing changes
- o 5.1.1.1 - 1. Identify the problem
- o 5.1.1.1.1 - Gather information from the user, identify user changes, and, if applicable, perform backups before making changes
- o 5.1.1.1.2 - Inquire regarding environmental or infrastructure changes
- o 5.1.1.2 - 2. Establish a theory of probable cause (question the obvious)
- o 5.1.1.2.1 - If necessary, conduct external or internal research based on symptoms
- o 5.1.1.3 - 3. Test the theory to determine the cause
- o 5.1.1.3.1 - Once the theory is confirmed, determine the next steps to resolve the problem
- o 5.1.1.3.2 - If the theory is not confirmed, re-establish a new theory or escalate
- o 5.1.1.4 - 4. Establish a plan of action to resolve the problem and implement the solution
- o 5.1.1.4.1 - Refer to the vendor's instructions for guidance
- o 5.1.1.5 - 5. Verify full system functionality and, if applicable, implement preventive measures
- o 5.1.1.6 - 6. Document the findings, actions, and outcomes

5.2	Given a scenario, troubleshoot problems related to motherboards, RAM, CPU, and power.
	
	    5.2.1 - Common symptoms
	        o 5.2.1.1 - Power-on self-test (POST) beeps
	        o 5.2.1.2 - Proprietary crash screens (blue screen of death [BSOD]/pinwheel)
	        o 5.2.1.3 - Black screen
	        o 5.2.1.4 - No power
	        o 5.2.1.5 - Sluggish performance
	        o 5.2.1.6 - Overheating
	        o 5.2.1.7 - Burning smell
	        o 5.2.1.8 - Intermittent shutdown
	        o 5.2.1.9 - Application crashes
	        o 5.2.1.10 - Grinding noise
	        o 5.2.1.11 - Capacitor swelling
	        o 5.2.1.12 - Inaccurate system date/time
		2.6
		3.4, 3.7, 3.10, 3.14
		
		12.7
		
		14.11

5.3	Given a scenario, troubleshoot and diagnose problems with storage drives and RAID arrays.
	
	    5.3.1 - Common symptoms
	        o 5.3.1.1 - Light-emitting diode (LED) status indicators
	        o 5.3.1.2 - Grinding noises
	        o 5.3.1.3 - Clicking sounds
	        o 5.3.1.4 - Bootable device not found
	        o 5.3.1.5 - Data loss/corruption
	        o 5.3.1.6 - RAID failure
	        o 5.3.1.7 - Self-monitoring, Analysis, and Reporting Technology (S.M.A.R.T) failure
	        o 5.3.1.8 - Extended read/write times
	        o 5.3.1.9 - Input/output operations per second (IOPS)
	        o 5.3.1.10 - Missing drives in OS
		5.3, 5.9
		10.5
		
		14.11

5.4	Given a scenario, troubleshoot video, projector, and display issues. 5.4.1 - Common symptoms	2.5 10.3

		o 5.4.1.1 - Incorrect data source o 5.4.1.2 - Physical cabling issues o 5.4.1.3 - Burned-out bulb o 5.4.1.4 - Fuzzy image o 5.4.1.5 - Display burn-in o 5.4.1.6 - Dead pixels o 5.4.1.7 - Flashing screen o 5.4.1.8 - Incorrect color display o 5.4.1.9 - Audio issues o 5.4.1.10 - Dim image o 5.4.1.11 - Intermittent projector shutdown	
5.5	Given a scenario, troubleshoot common issues with mobile devices. 5.5.1 - Common symptoms o 5.5.1.1 - Poor battery health o 5.5.1.2 - Swollen battery o 5.5.1.3 - Broken screen o 5.5.1.4 - Improper charging o 5.5.1.5 - Poor/no connectivity o 5.5.1.6 - Liquid damage o 5.5.1.7 - Overheating o 5.5.1.8 - Digitizer issues o 5.5.1.9 - Physically damaged ports o 5.5.1.10 - Malware o 5.5.1.11 - Cursor drift/touch calibration		12.7
5.6	Given a scenario, troubleshoot and resolve printer issues. 5.6.1 - Common symptoms o 5.6.1.1 - Lines down the printed pages o 5.6.1.2 - Garbled print o 5.6.1.3 - Toner not fusing to paper o 5.6.1.4 - Paper jams o 5.6.1.5 - Faded print		13.1, 13.2, 13.3, 13.4

		o 5.6.1.6 - Incorrect paper size o 5.6.1.7 - Paper not feeding o 5.6.1.8 - Multipage misfeed o 5.6.1.9 - Multiple prints pending in queue o 5.6.1.10 - Speckling on printed pages o 5.6.1.11 - Double/echo images on the print o 5.6.1.12 - Incorrect chroma display o 5.6.1.13 - Grinding noise o 5.6.1.14 - Finishing issues o 5.6.1.14.1 - Staple jams o 5.6.1.14.2 - Hole punch o 5.6.1.15 - Incorrect page orientation	
5.7	Given a scenario, troubleshoot problems with wired and wireless networks. 5.7.1 - Common symptoms o 5.7.1.1 - Intermittent wireless connectivity o 5.7.1.2 - Slow network speeds o 5.7.1.3 - Limited connectivity o 5.7.1.4 - Jitter o 5.7.1.5 - Poor Voice over Internet Protocol (VoIP) quality o 5.7.1.6 - Port flapping o 5.7.1.7 - High latency o 5.7.1.8 - External interference		2.5 11.9 12.7 13.2 14.11

Objective Mapping: LabSim Section to CompTIA 220-1102 Objectives

The TestOut PC Pro course covers the following CompTIA A+ Certification 220-1102 exam objectives:

Section	Title	Objectives

1.0	Course Introduction	
1.1	Course Introduction	4.5 - Summarize environmental impacts and local environmental controls. 　　　4.5.3 - Power surges, brownouts, and blackouts 　　　4.5.3.1 - Battery backup
2.0	**PC Technician Responsibilities**	
2.1	Protection and Safety	4.4 - Given a scenario, use common safety procedures. 　　　4.4.1 - Electrostatic discharge (ESD) straps 　　　4.4.2 - ESD mats 　　　4.4.3 - Equipment grounding 　　　4.4.4 - Proper power handling 　　　4.4.5 - Proper component handling and storage 　　　4.4.6 - Antistatic bags 　　　4.4.8 - Personal safety 　　　4.4.8.1 - Disconnect power before repairing PC 　　　4.4.8.2 - Lifting techniques 　　　4.4.8.3 - Electrical fire safety 　　　4.4.8.4 - Safety goggles 4.5 - Summarize environmental impacts and local environmental controls. 　　　4.5.1 - Material safety data sheet (MSDS)/documentation for handling and disposal 　　　4.5.1.1 - Proper battery disposal 　　　4.5.1.2 - Proper toner disposal 　　　4.5.1.3 - Proper disposal of other devices and assets

		4.5.2 - Temperature, humidity-level awareness, and proper ventilation

4.5.2.1 - Location/equipments placement
4.5.2.2 - Dust cleanup |
| 2.2 | Environmental Controls | 4.5 - Summarize environmental impacts and local environmental controls.

4.5.1 - Material safety data sheet (MSDS)/documentation for handling and disposal

4.5.1.1 - Proper battery disposal
4.5.1.2 - Proper toner disposal
4.5.1.3 - Proper disposal of other devices and assets

4.5.2 - Temperature, humidity-level awareness, and proper ventilation

4.5.2.1 - Location/equipments placement
4.5.2.2 - Dust cleanup
4.5.2.3 - Compressed air/vacuums

4.5.3 - Power surges, brownouts, and blackouts

4.5.3.1 - Battery backup
4.5.3.2 - Surge supressor |
| 2.3 | Professionalism | 4.7 - Given a scenario, use proper communication techniques and professionalism.

4.7.1 - Professional appearance and attire
4.7.2 - Use proper language and avoid jargon, acronyms, and slang, when applicable
4.7.3 - Maintain a positive attitude/project confidence
4.7.4 - Actively listen, take notes, and avoid interrupting the customer
4.7.5 - Be culturally sensitive
4.7.6 - Be on time (if late, contact the customer) |

		4.7.7 - Avoid distractions 4.7.8 - Dealing with difficult customers or situations 4.7.9 - Set and meet expectations/timeline and communicate status with the customer 4.7.10 - Deal appropriately with customers' confidential and private materials
2.4	Change Management	4.2 - Explain basic change-management best practices. 4.2.1 - Documented business processes 4.2.2 - Change management
2.5	PC Maintenance	4.5 - Summarize environmental impacts and local environmental controls. 4.5.2 - Temperature, humidity-level awareness, and proper ventilation 4.5.2.1 - Location/equipments placement 4.5.2.2 - Dust cleanup 4.5.2.3 - Compressed air/vacuums
2.6	PC and Networking Tools	4.4 - Given a scenario, use common safety procedures. 4.4.1 - Electrostatic discharge (ESD) straps 4.4.2 - ESD mats 4.4.5 - Proper component handling and storage
2.7	Troubleshooting Process Overview	
2.8	Support Systems	4.1 - Given a scenario, implement best practices associated with documentation and support systems information management.

		4.1.1 - Ticketing systems 4.1.1.1 - User information 4.1.1.2 - Device information 4.1.1.3 - Description of problems 4.1.1.4 - Categories 4.1.1.5 - Severity 4.1.1.6 - Escalation levels 4.1.1.7 - Clear, concise written communication 4.1.1.7.1 - Problem description 4.1.1.7.2 - Progress notes 4.1.1.7.3 Problem resolution 4.1.2 - Asset management 4.1.2.1 - Inventory lists 4.1.2.2 - Database system 4.1.2.3 - Asset tags and IDs 4.1.2.4 - Procurement life cycle 4.1.2.5 - Warranty and licensing 4.1.2.6 - Assigned users
2.9	Documentation	4.1 - Given a scenario, implement best practices associated with documentation and support systems information management. 4.1.3 - Types of documents 4.1.3.1 - Acceptable use policy (AUP) 4.1.3.2 - Network topology diagram 4.1.3.3 - Regulatory compliance requirements 4.1.3.3.1 - Splash screens 4.1.3.5 - Standard operating procedures 4.1.3.6 - New-user setup checklist 4.1.3.7 - End-user termination checklist

		4.1.4 - Knowledge base/articles
3.0	**Hardware**	
3.1	Network Media	
3.2	Cables and Connectors	
3.3	Cases and Motherboards	
3.4	Motherboard Troubleshooting	4.1 - Given a scenario, implement best practices associated with documentation and support systems information management. 4.1.1 - Ticketing systems 4.1.1.7 - Clear, concise written communication 4.1.1.7.2 - Progress notes 4.1.1.7.3 Problem resolution
3.5	Memory	1.7 - Given a scenario, apply application installation and configuration concepts. 1.7.1 - System requirements for applications 1.7.1.4 - RAM requirements
3.6	Memory Installation	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility. 1.4.5 - System 4.4 - Given a scenario, use common safety procedures. 4.4.1 - Electrostatic discharge (ESD) straps

		4.4.2 - ESD mats
3.7	Memory Troubleshooting	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility. 1.4.12 - Administrative Tools
3.8	BIOS/UEFI	3.2 - Given a scenario, troubleshoot common personal computer (PC) security issues. 3.2.1 - Common symptoms
3.9	Processors	
3.10	Processor Troubleshooting	
3.11	Video and Expansion Cards	
3.12	Audio	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility. 1.4.8 - Sound
3.13	Cooling	
3.14	Power Supplies	
4.0	**Operating Systems Basics**	
4.1	Operating System	1.8 - Explain common OS types and their purposes. 1.8.1 - Workstation OSs

		1.8.1.1 - Windows 1.8.1.2 - Linux 1.8.1.3 - macOS 1.8.1.4 - Chrome OS 1.8.4 - Vendor life-cycle limitations 1.8.4.1 - End-of-life (EOL) 1.8.4.2 - Update limitations 1.8.5 - Compatibility concerns between OSs
4.2	Windows Basics	1.1 - Identify basic features of Microsoft Windows editions. 1.1.1 - Windows 10 editions 1.1.1.1 - Home 1.1.1.2 - Pro 1.1.1.3 - Pro for Workstations 1.1.1.4 - Enterprise 1.1.2 - Feature differences 1.1.2.1 - Domain access vs. workgroup 1.1.2.2 - Desktop styles/user interface 1.1.2.3 - Availability of Remoter Desktop Protocol (RDP) 1.1.2.4 - Random-access memory (RAM) support limitations 1.1.2.5 - Bitlocker 1.1.2.6 - gpedit.msc 1.1.3 - Upgrade paths 1.1.3.1 - In-place upgrade

		1.8 - Explain common OS types and their purposes.
		1.8.1 - Workstation OSs

		1.8.1.1 - Windows
		        1.8.1.2 - Linux
		        1.8.1.3 - macOS

		1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment.
		1.9.2 - Types of installations

		1.9.2.1 - Upgrade
		        1.9.2.3 - Clean install
		        1.9.2.4 - Image deployment
		        1.9.2.5 - Repair installation

		3.1 - Given a scenario, troubleshoot common Windows OS problems.
		3.1.2 - Common troubleshooting steps
		3.1.2.7 - Repair Windows
4.3	Linux Basics	1.8 - Explain common OS types and their purposes.
		1.8.1 - Workstation OSs
		1.8.1.2 - Linux
		1.11 - Identify common features and tools of the Linux client/desktop OS.
		1.11.1 - Common commands

		1.11.1.1 - ls 1.11.1.3 - mv 1.11.1.4 - cp 1.11.1.14 - ps 1.11.1.16 - top 1.11.2 - Best practices 1.11.2.1 - Backups 1.11.2.2 - Antivirus 1.11.2.3 - Updates/patches 1.11.3 - Tools 1.11.3.1 - Shell/terminal 1.11.3.2 - Samba
4.4	macOS Basics	1.8 - Explain common OS types and their purposes. 1.8.3 - Various filesystem types 1.8.3.5 - Apple File System (APFS) 1.10 - Identify common features and tools of the macOS/desktop OS. 1.10.1 - Installation and uninstallation of applications 1.10.1.1.1 - .dmg 1.10.1.1.2 - .pkg 1.10.1.1.3 - .app 1.10.1.2 - App Store 1.10.1.3 - Uninstallation process 1.10.2 - Apple ID and corporate restrictions

		1.10.3 - Best practices 1.10.3.2 - Antivirus 1.10.3.3 - Updates/patches 1.10.5 - Features 1.10.5.1 - Multiple desktops 1.10.5.2 - Mission Control 1.10.5.3 - Keychain 1.10.5.4 - Spotlight 1.10.5.6 - Gestures 1.10.5.7 - Finder 1.10.5.8 - Remote Disc 1.10.5.9 - Dock 1.10.8 - Terminal 1.10.9 - Force Quit
5.0	**Storage**	
5.1	Storage Devices	
5.2	SATA	
5.3	Optical Media	
5.4	RAID	
5.5	File Systems	1.2 - Given a scenario, use the appropriate Microsoft command-line tool. 1.2.2 - Command-line tools

1.2.2.10 - format
1.2.2.19 - diskpart

1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

1.3.2 - Microsoft Management Console (MMC) snap-in

1.3.2.2 - Disk Management (diskmgmt.msc)
1.3.2.4 - Device Manager (devmgmt.msc)

1.8 - Explain common OS types and their purposes.

1.8.3 - Various filesystem types

1.8.3.1 - New Technology File System (NTFS)
1.8.3.2 - File Allocation Table 32 (FAT32)
1.8.3.3 - Third extended filesystem (ext3)
1.8.3.4 - Fourth extended filesystem (ext4)
1.8.3.6 - Extensible File Allocation Table (exFAT)

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

1.9.3 - Partitioning

1.9.3.1 - GUID [globally unique identifier]
1.9.3.2 - Partition Table (GPT)
1.9.3.3 - Master boot record (MBR)

1.9.4 - Drive format

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

		4.1.1 - Ticketing systems
		4.1.1.7 - Clear, concise written communication 4.1.1.7.2 - Progress notes 4.1.1.7.3 Problem resolution
5.6	Storage Management	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS). 1.3.2 - Microsoft Management Console (MMC) snap-in 1.3.2.2 - Disk Management (diskmgmt.msc)
5.7	Storage Spaces	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS). 1.3.2 - Microsoft Management Console (MMC) snap-in 1.3.2.2 - Disk Management (diskmgmt.msc)
5.8	Disk Optimization	1.2 - Given a scenario, use the appropriate Microsoft command-line tool. 1.2.2 - Command-line tools 1.2.2.6 - chkdsk 1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS). 1.3.3 - Additional tools 1.3.3.4 - Disk Cleanup (cleanmgr.exe)

		1.3.3.5 - Disk Defragment (dfrgui.exe)
		
		1.11 - Identify common features and tools of the Linux client/desktop OS.
		
		    1.11.1 - Common commands
		
		    1.11.1.2 - pwd
		    1.11.1.12 - df
		
		3.1 - Given a scenario, troubleshoot common Windows OS problems.
		
		    3.1.1 - Common symptoms
		
		    3.1.1.2 - Sluggish performance

5.9	Storage and RAID Troubleshooting	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		
		    1.3.3 - Additional tools
		
		    1.3.3.5 - Disk Defragment (dfrgui.exe)

6.0	**System Implementation**	

6.1	Windows Pre-Installation	1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment.
		
		    1.9.2 - Types of installations
		
		    1.9.2.1 - Upgrade
		    1.9.2.3 - Clean install
		    1.9.2.5 - Repair installation
		    1.9.2.7 - Other considerations

		1.9.2.7.1 - Third-party drivers 1.9.5 - Upgrade considerations 1.9.5.1 - Backup files and user preferences 1.9.5.2 - Application and driver support/backward compatibility 1.9.5.3 - Hardware compatibility
6.2	Windows Installation	1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment. 1.9.1 - Boot methods 1.9.1.1 - USB 1.9.1.2 - Optical media 1.9.1.3 - Network 1.9.1.4 - Solid-state/flash drives 1.9.1.5 - Internet-based 1.9.1.6 - External/hot-swappable drive 1.9.1.7 - Internal hard drive (partition) 1.9.2 - Types of installations 1.9.2.1 - Upgrade 1.9.2.2 - Recovery partition 1.9.2.3 - Clean install 1.9.2.4 - Image deployment 1.9.2.5 - Repair installation 1.9.2.6 - Remote network installation 1.9.2.7 - Other considerations 1.9.2.7.1 - Third-party drivers 1.9.4 - Drive format

		4.1 - Given a scenario, implement best practices associated with documentation and support systems information management. 4.1.1 - Ticketing systems 4.1.1.7 - Clear, concise written communication 4.1.1.7.2 - Progress notes 4.1.1.7.3 Problem resolution
6.3	Cloud Computing	
6.4	Virtualization	
7.0	**System Management 1**	
7.1	Windows System Tools	1.2 - Given a scenario, use the appropriate Microsoft command-line tool. 1.2.1 - Navigation 1.2.1.1 - cd 1.2.1.2 - dir 1.2.1.3 - md 1.2.1.4 - rmdir 1.2.1.5 - Drive navigation inputs 1.2.1.5.1 - C:\ or D:\ or x:\ 1.2.2 - Command-line tools 1.2.2.1 - ipconfig 1.2.2.2 - ping 1.2.2.3 - hostname 1.2.2.4 - netstat 1.2.2.5 - nslookup 1.2.2.6 - chkdsk

		1.2.2.7 - net user
		1.2.2.8 - net use
		1.2.2.9 - tracert
		1.2.2.10 - format
		1.2.2.11 - xcopy
		1.2.2.12 - copy
		1.2.2.13 - robocopy
		1.2.2.14 - gpupdate
		1.2.2.15 - gpresult
		1.2.2.16 - shutdown
		1.2.2.17 - sfc
		1.2.2.18 - [command name] /?
		1.2.2.19 - diskpart
		1.2.2.20 - pathping
		1.2.2.21 - winver
		1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		1.3.1 - Task Manager
		1.3.1.1 - Services
		1.3.1.2 - Startup
		1.3.1.3 - Performance
		1.3.1.4 - Processes
		1.3.1.5 - Users
		1.3.2 - Microsoft Management Console (MMC) snap-in
		1.3.2.1 - Event viewer (eventvwr.msc)
		1.3.2.2 - Disk Management (diskmgmt.msc)
		1.3.2.3 - Task Scheduler (taskschdd.msc)
		1.3.2.4 - Device Manager (devmgmt.msc)
		1.3.2.5 - Certificate Manager (certmgr.msc)
		1.3.2.6 - Local Users and Groups (lusrmgr.msc)
		1.3.2.7 - Performance Monitor (perfmon.msc)

1.3.2.8 - Group Policy Editor (gpedit.msc)

1.3.3 - Additional tools

1.3.3.1 - System Information (msinfo32.exe)
1.3.3.3 - System Configuration (msconfig.exe)
1.3.3.5 - Disk Defragment (dfrgui.exe)
1.3.3.6 - Registry Editor (regedit.exe)

1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

1.4.1 - Internet Options
1.4.2 - Devices and Printers
1.4.3 - Programs and Features
1.4.4 - Network and Sharing center
1.4.5 - System
1.4.6 - Windows Defender Firewall
1.4.7 - Mail
1.4.8 - Sound
1.4.9 - User Accounts
1.4.10 - Device Manager
1.4.11 - Indexing Options
1.4.12 - Administrative Tools
1.4.13 - File Explorer Options

1.4.13.1 - Show hidden files
1.4.13.2 - Hide extensions
1.4.13.3 - General options
1.4.13.4 - View options

1.4.14 - Power Options

1.4.14.1 - Hibernate
1.4.14.3 - Sleep/suspend
1.4.14.5 - Choose what closing the lid does

		1.4.15 - Ease of Access 4.9 - Given a scenario, use remote access technologies. 4.9.1 - Methods/tools 4.9.1.6 - Microsoft Remote Assistance (MSRA)
7.2	Windows Settings	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility. 1.4.11 - Indexing Options 1.5 - Given a scenario, use the appropriate Windows settings. 1.5.1 - Time and Language 1.5.2 - Update and Security 1.5.3 - Personalization 1.5.4 - Apps 1.5.5 - Privacy 1.5.6 - System 1.5.7 - Devices 1.5.8 - Network and Internet 1.5.9 - Gaming 1.5.10 - Accounts
7.3	Performance Monitoring	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS). 1.3.1 - Task Manager 1.3.1.1 - Services 1.3.1.2 - Startup 1.3.1.3 - Performance 1.3.1.4 - Processes

		1.3.1.5 - Users
		1.3.2 - Microsoft Management Console (MMC) snap-in
		1.3.2.1 - Event viewer (eventvwr.msc)
		1.3.2.7 - Performance Monitor (perfmon.msc)
		1.3.3 - Additional tools
		1.3.3.2 - Resource Monitor (resmon.exe)
7.4	Windows Application Management	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		1.3.2 - Microsoft Management Console (MMC) snap-in
		1.3.2.3 - Task Scheduler (taskschdd.msc)
		1.7 - Given a scenario, apply application installation and configuration concepts.
		1.7.1 - System requirements for applications
		1.7.1.1 - 32-bit vs. 64-bit dependent application requirements
		1.7.1.2 - Dedicated graphics card vs. integrated
		1.7.1.3 - Video random-access memory (VRAM) requirements
		1.7.1.4 - RAM requirements
		1.7.1.5 - Central processing unit (CPU) requirements
		1.7.1.6 - External hardware tokens
		1.7.1.7 - Storage requirements
		1.7.2 - OS requirements for applications
		1.7.2.1 - Application to OS compatibility

		1.7.2.2 - 32-bit vs. 64-bit OS
		1.7.3 - Distribution methods
		1.7.3.1 - Physical media vs. downloadable
		1.7.3.2 - ISO mountable
		1.7.4 - Other considerations for new applications
		1.7.4.1 - Impact to device
		1.7.4.2 - Impact to network
		1.7.4.3 - Impact to operation
		1.7.4.4 - Impact to business
		1.10 - Identify common features and tools of the macOS/desktop OS.
		1.10.1 - Installation and uninstallation of applications
		1.10.1.2 - App Store
7.5	Linux Application Management	**1.11 - Identify common features and tools of the Linux client/desktop OS.**
		1.11.1 - Common commands
		1.11.1.9 - apt-get
		1.11.1.10 - yum
		1.11.1.14 - ps
		1.11.2 - Best practices
		1.11.2.3 - Updates/patches
		1.11.3 - Tools

		1.11.3.1 - Shell/terminal
7.6	Digital Content Management	4.6 - Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts. 4.6.2 - Licensing/digital rights management (DRM)/end-user license agreement (EULA) 4.6.2.1 - Valid licenses 4.6.2.2 - Non-expired licenses 4.6.2.3 - Personal use license vs. corporate use license 4.6.2.4 - Open-source license
7.7	Virtual Memory	
7.8	Windows and Application Troubleshooting	3.1 - Given a scenario, troubleshoot common Windows OS problems. 3.1.1 - Common symptoms 3.1.1.1 - Blue screen of death (BSOD) 3.1.1.2 - Sluggish performance 3.1.1.3 - Boot problems 3.1.1.5 - Services not starting 3.1.1.6 - Applications crashing 3.1.1.7 - Low memory warnings 3.1.1.8 - USB controller resource warnings 3.1.1.9 - System instability 3.1.1.10 - No OS found 3.1.1.11 - Slow profile load 3.1.1.12 - Time drift 3.1.2 - Common troubleshooting steps 3.1.2.1 - Reboot

		3.1.2.2 - Restart services 3.1.2.3 - Uninstall/reinstall/update applications 3.1.2.4 - Add resources 3.1.2.5 - Verify requirements 3.1.2.6 - System file check 3.1.2.7 - Repair Windows 3.1.2.8 - Restore 3.1.2.9 - Reimage 3.1.2.10 - Roll back updates 3.1.2.11 - Rebuild Windows profiles
7.9	Scripting Basics	4.8 - Identify the basics of scripting. 4.8.1 - Script file types 4.8.1.1 - .bat 4.8.1.2 - .ps1 4.8.1.3 - .vbs 4.8.1.4 - .sh 4.8.1.5 - .js 4.8.1.6 - .py 4.8.2 - Use cases for scripting 4.8.2.1 - Basic automation 4.8.2.2 - Restarting machines 4.8.2.3 - Remapping network drives 4.8.2.4 - Installation of applications 4.8.2.5 - Automated backups 4.8.2.6 - Gathering of information/data 4.8.2.7 - Initiating updates 4.8.3 - Other considerations when using scripts 4.8.3.1 - Unintentionally introducing malware 4.8.3.2 - Inadvertently changing system settings

		4.8.3.3 - Browser or system crashes due to mishandling of resources
8.0	**System Management 2**	
8.1	Active Directory	1.1 - Identify basic features of Microsoft Windows editions.
		1.1.2 - Feature differences
		1.1.2.1 - Domain access vs. workgroup
		1.2 - Given a scenario, use the appropriate Microsoft command-line tool.
		1.2.2 - Command-line tools
		1.2.2.14 - gpupdate 1.2.2.15 - gpresult
		1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		1.3.2 - Microsoft Management Console (MMC) snap-in
		1.3.2.8 - Group Policy Editor (gpedit.msc)
		2.1 - Summarize various security measures and their purposes.
		2.1.5 - Active Directory
		2.1.5.1 - Login script 2.1.5.2 - Domain 2.1.5.3 - Group Policy/updates 2.1.5.4 - Organizational units 2.1.5.7 - Security groups

8.2	Users and Groups	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		1.3.2 - Microsoft Management Console (MMC) snap-in
		1.3.2.6 - Local Users and Groups (lusrmgr.msc)
		1.5 - Given a scenario, use the appropriate Windows settings.
		1.5.10 - Accounts
		2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
		2.5.3 - Users and groups
		2.5.3.1 - Local vs. Microsoft account 2.5.3.2 - Standard account 2.5.3.3 - Administrator 2.5.3.4 - Guest user 2.5.3.5 - Power user
		2.5.4 - Login OS options
		2.5.4.1 - Username and password 2.5.4.2 - Personal identification number (PIN) 2.5.4.3 - Fingerprint 2.5.4.4 - Facial recognition 2.5.4.5 - Single sign-on (SSO)
		2.5.6 - Run administrator vs. standard user
		2.5.6.1 - User Account Control (UAC)

		2.5.7 - Bitlocker
8.3	Remote Services	4.9 - Given a scenario, use remote access technologies. 4.9.1 - Methods/tools 4.9.1.1 - RDP 4.9.1.4 - Secure Shell (SSH) 4.9.1.5 - Remote monitoring and management (RMM) 4.9.1.6 - Microsoft Remote Assistance (MSRA) 4.9.1.7 - Third-party tools 4.9.1.7.1 - Screen-sharing software 4.9.1.7.2 - Video-conferencing software 4.9.1.7.3 - File transfer software 4.9.1.7.4 - Desktop management software 4.9.2 - Security considerations of each access method
8.4	VPN	4.9 - Given a scenario, use remote access technologies. 4.9.1 - Methods/tools 4.9.1.2 - VPN
8.5	Updates	1.5 - Given a scenario, use the appropriate Windows settings. 1.5.2 - Update and Security 3.2 - Given a scenario, troubleshoot common personal computer (PC) security issues. 3.2.1 - Common symptoms

		3.2.1.6 - OS update failures
8.6	System Backup	1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment. 1.9.5 - Upgrade considerations 1.9.5.1 - Backup files and user preferences 1.10 - Identify common features and tools of the macOS/desktop OS. 1.10.4 - System Preferences 1.10.4.7 - Time Machine 1.11 - Identify common features and tools of the Linux client/desktop OS. 1.11.2 - Best practices 1.11.2.1 - Backups 4.3 - Given a scenario, implement workstation backup and recovery methods. 4.3.1 - Backup and recovery 4.3.1.1 - Full 4.3.1.2 - Incremental 4.3.1.3 - Differential 4.3.1.4 - Synthetic 4.3.2 - Backup testing 4.3.2.1 - Frequency

		4.3.3 - Backup rotation schemes 4.3.3.1 - On site vs. off site 4.3.3.2 - Grandfather-father-son (GFS) 4.3.3.3 - 3-2-1 backup rule
8.7	System Recovery	2.3 - Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods. 2.3.2 - Tools and methods 2.3.2.1 - Recovery console 2.3.2.7 - OS reinstallation 3.1 - Given a scenario, troubleshoot common Windows OS problems. 3.1.2 - Common troubleshooting steps 3.1.2.2 - Restart services 3.1.2.7 - Repair Windows 3.1.2.8 - Restore 3.1.2.9 - Reimage 3.1.2.10 - Roll back updates
8.8	Windows Boot Errors	1.2 - Given a scenario, use the appropriate Microsoft command-line tool. 1.2.2 - Command-line tools 1.2.2.17 - sfc 3.1 - Given a scenario, troubleshoot common Windows OS problems. 3.1.1 - Common symptoms

		3.1.1.3 - Boot problems
		3.1.2 - Common troubleshooting steps
		3.1.2.1 - Reboot 3.1.2.8 - Restore
9.0	**File Management**	
9.1	Manage Files on Windows	1.2 - Given a scenario, use the appropriate Microsoft command-line tool.
		1.2.1 - Navigation
		1.2.1.1 - cd 1.2.1.2 - dir 1.2.1.3 - md 1.2.1.4 - rmdir 1.2.1.5 - Drive navigation inputs 1.2.1.5.1 - C:\ or D:\ or x:\
		1.2.2 - Command-line tools
		1.2.2.11 - xcopy 1.2.2.12 - copy 1.2.2.13 - robocopy
		1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
		1.4.13 - File Explorer Options
		1.4.13.1 - Show hidden files 1.4.13.2 - Hide extensions

		1.8 - Explain common OS types and their purposes. 1.8.1 - Workstation OSs 1.8.1.1 - Windows 2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS. 2.5.5 - NTFS vs. share permissions 2.5.5.1 - File and folder attributes
9.2	NTFS and Share Permissions	2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS. 2.5.5 - NTFS vs. share permissions 2.5.5.1 - File and folder attributes 2.5.5.2 - Inheritance
9.3	File Encryption	2.2 - Compare and contrast wireless security protocols and authentication methods. 2.2.1 - Protocols and encryption 2.2.1.1 - WiFi Protected Access 2 (WPA2) 2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS. 2.5.5 - NTFS vs. share permissions

		2.5.5.1 - File and folder attributes 2.5.7 - Bitlocker 2.5.8 - Bitlocker To Go 2.5.9 - Encrypting File System (EFS) **2.6 - Given a scenario, configure a workstation to meet best practices for security.** 2.6.1 - Data-at-rest encryption
9.4	Linux File Management	**1.8 - Explain common OS types and their purposes.** 1.8.3 - Various filesystem types 1.8.3.1 - New Technology File System (NTFS) 1.8.3.2 - File Allocation Table 32 (FAT32) 1.8.3.3 - Third extended filesystem (ext3) 1.8.3.4 - Fourth extended filesystem (ext4) 1.8.3.6 - Extensible File Allocation Table (exFAT) **1.11 - Identify common features and tools of the Linux client/desktop OS.** 1.11.1 - Common commands 1.11.1.1 - ls 1.11.1.2 - pwd 1.11.1.3 - mv 1.11.1.4 - cp 1.11.1.5 - rm 1.11.1.6 - chmod 1.11.1.7 - chown 1.11.1.8 - su/sudo 1.11.1.11 - ip 1.11.1.13 - grep 1.11.1.15 - man

		1.11.1.17 - find 1.11.1.19 - cat
10.0	**Peripheral Devices**	
10.1	Peripheral Devices	1.5 - Given a scenario, use the appropriate Windows settings. 1.5.7 - Devices 1.5.9 - Gaming 1.10 - Identify common features and tools of the macOS/desktop OS. 1.10.4 - System Preferences 1.10.4.4 - Scanners
10.2	Display Devices	1.10 - Identify common features and tools of the macOS/desktop OS. 1.10.4 - System Preferences 1.10.4.1 - Displays
10.3	Display, Video, and Projector Troubleshooting	
10.4	Device Driver Management	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS). 1.3.2 - Microsoft Management Console (MMC) snap-in 1.3.2.4 - Device Manager (devmgmt.msc)

		1.3.3 - Additional tools
		1.3.3.1 - System Information (msinfo32.exe) 1.3.3.3 - System Configuration (msconfig.exe)
		1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
		1.4.2 - Devices and Printers 1.4.10 - Device Manager
		1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment.
		1.9.5 - Upgrade considerations
		1.9.5.2 - Application and driver support/backward compatibility
		1.10 - Identify common features and tools of the macOS/desktop OS.
		1.10.3 - Best practices
		1.10.3.3 - Updates/patches
		1.10.6 - Disk Utility
		1.11 - Identify common features and tools of the Linux client/desktop OS.
		1.11.2 - Best practices
10.5	Device Driver Troubleshooting	1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
		1.3.2 - Microsoft Management Console (MMC) snap-in

		1.3.2.4 - Device Manager (devmgmt.msc)
		1.3.3 - Additional tools
		1.3.3.3 - System Configuration (msconfig.exe)
		1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
		1.4.10 - Device Manager
		1.9 - Given a scenario, perform OS installations and upgrades in a diverse OS environment.
		1.9.2 - Types of installations
		1.9.2.7.1 - Third-party drivers
		3.1 - Given a scenario, troubleshoot common Windows OS problems.
		3.1.2 - Common troubleshooting steps
		3.1.2.3 - Uninstall/reinstall/update applications 3.1.2.7 - Repair Windows 3.1.2.8 - Restore 3.1.2.10 - Roll back updates
11.0	**Networking**	
11.1	Networking Overview	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop.
		1.6.3 - Client network configuration

		1.6.3.3 - Subnet mask
11.2	Networking Ports and Protocols	
11.3	Client-Side Network Configuration	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop. 1.6.3 - Client network configuration 1.6.3.1 - Internet Protocol (IP) addressing scheme 1.6.3.2 - Domain Name System (DNS) settings 1.6.3.3 - Subnet mask 1.6.3.4 - Gateway 1.6.3.5 - Static vs. dynamic 1.6.6 - Public network vs. private network
11.4	Services Provided by Network Devices	
11.5	Wireless Networking	2.2 - Compare and contrast wireless security protocols and authentication methods. 2.2.1 - Protocols and encryption 2.2.1.1 - WiFi Protected Access 2 (WPA2) 2.2.1.2 - WPA3 2.2.1.3 - Temporal Key Integrity Protocol (TKIP) 2.2.1.4 - Advanced Encryption Standard (AES) 2.2.2 - Authentication 2.2.2.1 - Remote Authentication Dial-In User Service (RADIUS) 2.2.2.2 - Terminal Access Controller Access-Control System (TACACS+) 2.2.2.3 - Kerberos

		2.2.2.4 - Multifactor
11.6	SOHO Configuration	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop. 1.6.6 - Public network vs. private network 2.9 - Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks. 2.9.1 - Home router settings 2.9.1.1 - Change default passwords 2.9.1.2 - IP filtering 2.9.1.3 - Firmware updates 2.9.1.4 - Content filtering 2.9.1.5 - Physical placement/secure locations 2.9.1.6 - Dynamic Host Configuration Protocol (DHCP) reservations 2.9.1.7 - Static wide-area network (WAN) IP 2.9.1.8 - Universal Plug and Play (UPnP) 2.9.1.9 - Screened subnet 2.9.2 - Wireless specific 2.9.2.1 - Changing the service set identifier (SSID) 2.9.2.2 - Disabling SSID broadcast 2.9.2.3 - Encryption settings 2.9.2.4 - Disabling guest access 2.9.2.5 - Changing channels 2.9.3 - Firewall settings 2.9.3.1 - Disabling unused ports 2.9.3.2 - Port forwarding/mapping

11.7	Networking Hardware	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop.
		1.6.4 - Establish network connections
		1.6.4.1 - Virtual private network (VPN)
		1.6.4.2 - Wireless
		1.6.4.3 - Wired
		1.6.4.4 - Wireless wide area network (WWAN)
11.8	Command Line Network Utilities	1.2 - Given a scenario, use the appropriate Microsoft command-line tool.
		1.2.2 - Command-line tools
		1.2.2.1 - ipconfig
		1.2.2.2 - ping
		1.2.2.3 - hostname
		1.2.2.4 - netstat
		1.2.2.5 - nslookup
		1.2.2.6 - chkdsk
		1.2.2.7 - net user
		1.2.2.8 - net use
		1.2.2.9 - tracert
		1.2.2.20 - pathping
		1.11 - Identify common features and tools of the Linux client/desktop OS.
		1.11.1 - Common commands
		1.11.1.11 - ip
		1.11.1.18 - dig
11.9	Network Troubleshooting	1.2 - Given a scenario, use the appropriate Microsoft command-line tool.

		1.2.2 - Command-line tools 1.2.2.1 - ipconfig 1.2.2.2 - ping 4.1 - Given a scenario, implement best practices associated with documentation and support systems information management. 4.1.1 - Ticketing systems 4.1.1.1 - User information 4.1.1.2 - Device information 4.1.1.3 - Description of problems 4.1.1.4 - Categories 4.1.1.5 - Severity 4.1.1.6 - Escalation levels 4.1.1.7 - Clear, concise written communication 4.1.1.7.1 - Problem description 4.1.1.7.2 - Progress notes 4.1.1.7.3 Problem resolution
12.0	**Mobile Devices**	
12.1	Laptops	
12.2	Mobile Device Displays and Components	
12.3	Laptop Power Management	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility. 1.4.14 - Power Options 1.4.14.1 - Hibernate 1.4.14.2 - Power plans 1.4.14.3 - Sleep/suspend

		1.4.14.4 - Standby 1.4.14.5 - Choose what closing the lid does 1.4.14.6 - Turn on fast startup 1.4.14.7 - Universal Serial Bus (USB) selective suspend 3.4 - Given a scenario, troubleshoot common mobile OS and application issues. 3.4.1 - Common symptoms 3.4.1.6 - Battery life issues
12.4	Mobile Devices	1.8 - Explain common OS types and their purposes. 1.8.2 - Cell phone/tablet OSs 1.8.2.1 - iPadOS 1.8.2.2 - iOS 1.8.2.3 - Android
12.5	Mobile Device Network Connectivity	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop. 1.6.8 - Metered connections and limitations
12.6	Mobile Device Security	2.1 - Summarize various security measures and their purposes. 2.1.4 - Mobile device management (MDM) 2.2 - Compare and contrast wireless security protocols and authentication methods. 2.2.2 - Authentication

		2.2.2.4 - Multifactor **2.7 - Explain common methods for securing mobile and embedded devices.** 2.7.1 - Screen locks 2.7.1.1 - Facial recognition 2.7.1.2 - PIN codes 2.7.1.3 - Fingerprint 2.7.1.4 - Pattern 2.7.1.5 - Swipe 2.7.2 - Remote wipes 2.7.3 - Locator applications 2.7.4 - OS updates 2.7.5 - Device encryption 2.7.6 - Remote backup applications 2.7.7 - Failed login attempts restrictions 2.7.8 - Antivirus/anti-malware 2.7.9 - Firewalls 2.7.10 - Policies and procedures 2.7.10.1 - BYOD vs. corporate owned 2.7.10.2 - Profile security requirements 2.7.11 - Internet of Things (IoT)	
12.7	Laptop and Mobile Device Troubleshooting	**1.10 - Identify common features and tools of the macOS/desktop OS.** 1.10.5 - Features 1.10.5.5 - iCloud	

13.0	Printing	
13.1	Printer Overview	4.5 - Summarize environmental impacts and local environmental controls. 4.5.2 - Temperature, humidity-level awareness, and proper ventilation 4.5.2.2 - Dust cleanup
13.2	Print Connectivity	
13.3	Printer Types and Components	
13.4	Printer Troubleshooting	
14.0	Security	
14.1	Security Best Practices	2.1 - Summarize various security measures and their purposes. 2.1.3 - Logical security 2.1.3.1 - Principle of least privilege 2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS. 2.5.7 - Bitlocker 2.6 - Given a scenario, configure a workstation to meet best practices for security. 2.6.1 - Data-at-rest encryption 2.6.2 - Password best practices

| | | | 2.6.2.1 - Complexity requirements
2.6.2.1.1 - Length
2.6.2.1.2 - Character types
2.6.2.2 - Expiration requirements
2.6.2.3 - Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords

2.6.3 - End-user best practices

2.6.3.1 - Use screensaver locks
2.6.3.2 - Log off when not in use
2.6.3.3 - Secure/protect critical hardware (e.g., laptops)
2.6.3.4 - Secure personally identifiable information (PII) and passwords

2.6.4 - Account management

2.6.4.1 - Restrict user permissions
2.6.4.2 - Restrict login times
2.6.4.3 - Disable guest account
2.6.4.4 - Use failed attempts lockout
2.6.4.5 - Use timeout/screen lock

2.6.5 - Change default administrator's user account/password
2.6.6 - Disable AutoRun |
| 14.2 | | Incident Response and Regulated Data | 4.6 - Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.

4.6.1 - Incident response

4.6.1.1 - Chain of custody
4.6.1.2 - Inform management/law enforcement as necessary
4.6.1.3 - Copy of drive (data integrity and preservation)
4.6.1.4 - Documentation of incident |

		4.6.3 - Regulated data 4.6.3.1 - Credit card transactions 4.6.3.2 - Personal government-issued information 4.6.3.3 - PII 4.6.3.4 - Healthcare data 4.6.3.5 - Data retention requirements
14.3	Physical Security	2.1 - Summarize various security measures and their purposes. 2.1.1 - Physical security 2.1.1.1 - Access control vestibule 2.1.1.2 - Badge reader 2.1.1.3 - Video surveillance 2.1.1.4 - Alarm systems 2.1.1.5 - Motion sensors 2.1.1.6 - Door locks 2.1.1.7 - Equipment locks 2.1.1.8 - Guards 2.1.1.9 - Bollards 2.1.1.10 - Fences 2.1.2 - Physical security for staff 2.1.2.4 - Biometrics 2.1.2.4.2 - Fingerprint scanner 2.1.2.6 - Magnetometers
14.4	Logical Security Measures	2.1 - Summarize various security measures and their purposes. 2.1.3 - Logical security 2.1.3.1 - Principle of least privilege 2.1.3.2 - Access control lists (ACLs)

		2.1.3.3 - Multifactor authentication (MFA) 2.1.3.4 - Email 2.1.3.5 - Hard token 2.1.3.6 - Soft token 2.1.3.7 - Short message service (SMS) 2.1.3.8 - Voice call 2.1.3.9 - Authenticator application
14.5	Social Engineering Attacks	2.4 - Explain common social-engineering attacks, threats, and vulnerabilities. 2.4.1 - Social engineering 2.4.1.1 - Phishing 2.4.1.2 - Vishing 2.4.1.3 - Shoulder Surfing 2.4.1.4 - Whaling 2.4.1.5 - Tailgating 2.4.1.6 - Impersonation 2.4.1.7 - Dumpster diving 2.4.1.8 - Evil twin 2.4.2 - Threats 2.4.2.1 - Distributed denial of service (DDoS) 2.4.2.2 - Denial of service (DoS) 2.4.2.3 - Zero-day attack 2.4.2.4 - Spoofing 2.4.2.5 - On-path attack 2.4.2.6 - Brute-force attack 2.4.2.7 - Dictionary attack 2.4.2.8 - Insider threat 2.4.2.9 - Structured Query Language (SQL) injection 2.4.2.10 - Cross-site scripting (XSS) 2.4.3 - Vulnerabilities

		2.4.3.1 - Non-compliant systems 2.4.3.2 - Unpatched systems 2.4.3.3 - Unprotected systems (missing antivirus/missing firewall) 2.4.3.4 - EOL OSs 2.4.3.5 Bring your own device (BYOD)
14.6	Data Destruction and Disposal	2.8 - Given a scenario, use common data destruction and disposal methods. 2.8.1 - Physical destruction 2.8.1.1 - Drilling 2.8.1.2 - Shredding 2.8.1.3 - Degaussing 2.8.1.4 - Incinerating 2.8.2 - Recycling or repurposing best practices 2.8.2.1 - Erasing/wiping 2.8.2.2 - Low-level formatting 2.8.2.3 - Standard formatting 2.8.3 - Outsourcing concepts 2.8.3.1 - Third-party vendor 2.8.3.2 - Certification of destruction/recycling
14.7	Malware Protection	2.3 - Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods. 2.3.1 - Malware 2.3.1.1 - Trojan 2.3.1.2 - Rootkit 2.3.1.3 - Virus

| | | 2.3.1.4 - Spyware
2.3.1.5 - Ransomware
2.3.1.6 - Keylogger
2.3.1.7 - Boot sector virus
2.3.1.8 - Cryptominers

2.3.2 - Tools and methods

2.3.2.1 - Recovery console
2.3.2.2 - Antivirus
2.3.2.3 - Anti-malware
2.3.2.4 - Software firewalls
2.3.2.5 - Anti-phishing training
2.3.2.6 - User education regarding common threats
2.3.2.7 - OS reinstallation

2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.

2.5.1 - Defender Antivirus

2.5.1.1 - Activate/deactivate
2.5.1.2 - Updated definitions

3.3 - Given a scenario, use best practice procedures for malware removal.

3.3.1 - Investigate and verify malware symptoms
3.3.2 - Quarantine infected systems
3.3.3 - Disable System Restore in Windows
3.3.4 - Remediate infected systems

3.3.4.1 - Update anti-malware software
3.3.4.2 - Scanning and removal techniques (e.g., safe mode, preinstallation environment)

3.3.5 - Schedule scans and run updates |

		3.3.6 - Enable System Restore and create a restore point in Windows 3.3.7 - Educate the end user

14.8	Firewalls	1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
		
		      1.4.6 - Windows Defender Firewall
		
		1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop.
		
		      1.6.2 - Local OS firewall settings
		
		      1.6.2.1 - Application restrictions and exceptions
		      1.6.2.2 - Configuration
		
		2.3 - Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
		
		      2.3.2 - Tools and methods
		
		      2.3.2.4 - Software firewalls
		
		2.5 - Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
		
		      2.5.2 - Firewall
		
		      2.5.2.1 - Activate/deactivate
		      2.5.2.2 - Port security
		      2.5.2.3 - Application security

14.9	Proxy Servers	1.6 - Given a scenario, configure Microsoft Windows networking features on a client/desktop.

		1.6.5 - Proxy settings
14.10	Install, Configure, and Secure Browsers	2.10 - Given a scenario, install and configure browsers and relevant security settings. 2.10.1 - Browser download/installation 2.10.1.1 - Trusted sources 2.10.1.1.1 - Hashing 2.10.1.2 - Untrusted sources 2.10.2 - Extensions and plug-ins 2.10.2.1 - Trusted sources 2.10.2.2 - Untrusted sources 2.10.3 - Passwords managers 2.10.4 - Secure connections/sites - valid certificates 2.10.5 - Settings 2.10.5.1 - Pop-up blocker 2.10.5.2 - Clearing browsing data 2.10.5.3 - Clearing cache 2.10.5.4 - Private-browsing mode 2.10.5.5 - Sign-in/browser data synchronization 2.10.5.6 - Ad blockers
14.11	Security Troubleshooting	3.2 - Given a scenario, troubleshoot common personal computer (PC) security issues. 3.2.1 - Common symptoms 3.2.1.1 - Unable to access the network 3.2.1.2 - Desktop alerts 3.2.1.3 - False alerts regarding antivirus protection 3.2.1.4 - Altered system or personal files

		3.2.1.5 - Unwanted notifications within the OS 3.2.1.6 - OS update failures 3.2.2 - Browser-related symptoms 3.2.2.1 Random/frequent pop-ups 3.2.2.2 Certificate warnings 3.2.2.3 Redirection **3.5 - Given a scenario, troubleshoot common mobile OS and application security issues.** 3.5.1 - Security concerns 3.5.1.1 - Android package (APK) source 3.5.1.2 - Developer mode 3.5.1.3 - Root access/jailbreak 3.5.1.4 - Bootleg/malicious application 3.5.2 - Common symptoms 3.5.2.2 - Sluggish response time 3.5.2.3 - Data-usage limit notification 3.5.2.4 - Limited Internet connectivity 3.5.2.5 - No Internet connectivity 3.5.2.7 - Fake security warnings
15.0	**Capstone Exercises**	
		1.1 - Identify basic features of Microsoft Windows editions. 1.1.1 - Windows 10 editions

1.3 - Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).

      1.3.1 - Task Manager

      1.3.1.2 - Startup
      1.3.1.5 - Users

1.4 - Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.

      1.4.5 - System

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

      1.6.4 - Establish network connections

      1.6.4.2 - Wireless

1.11 - Identify common features and tools of the Linux client/desktop OS.

      1.11.1 - Common commands

2.6 - Given a scenario, configure a workstation to meet best practices for security.

      2.6.4 - Account management

      2.6.4.4 - Use failed attempts lockout
      2.6.4.5 - Use timeout/screen lock

2.9 - Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.

		2.9.1 - Home router settings
A.0	**TestOut PC Pro - Practice Exams**	
A.1	Prepare for TestOut PC Pro Certification	
A.2	TestOut PC Pro Exam Domain Review	
A.3	TestOut PC Pro Certification Practice Exam	
B.0	**CompTIA A+ Core 1 (220-1101) - Practice Exams**	
B.1	Prepare for CompTIA A+ Core 1 (220-1101) Certification	
B.2	CompTIA A+ Core 1 (220-1101) Domain Review (20 Questions)	
B.3	CompTIA A+ Core 1 (220-1101) Domain Review (All Questions)	
C.0	**CompTIA A+ Core 2 (220-1102) - Practice Exams**	
C.1	Prepare for CompTIA A+ Core 2 (220-1102) Certification	

C.2	CompTIA A+ Core 2 (220-1102) Domain Review (20 Questions)	
C.3	CompTIA A+ Core 2 (220-1102) Domain Review (All Questions)	

Objective Mapping: CompTIA 220-1102 Objectives to LabSim Section

The TestOut PC Pro course and certification exam cover the following CompTIA A+ Certification 220-1102 objectives:

#	Domain	Module.Section
1.0	**Operating Systems**	
1.1	Identify basic features of Microsoft Windows editions. 1.1.1 - Windows 10 editions o 1.1.1.1 - Home o 1.1.1.2 - Pro o 1.1.1.3 - Pro for Workstations o 1.1.1.4 - Enterprise 1.1.2 - Feature differences o 1.1.2.1 - Domain access vs. workgroup o 1.1.2.2 - Desktop styles/user interface o 1.1.2.3 - Availability of Remoter Desktop Protocol (RDP) o 1.1.2.4 - Random-access memory (RAM) support limitations o 1.1.2.5 - Bitlocker o 1.1.2.6 - gpedit.msc 1.1.3 - Upgrade paths o 1.1.3.1 - In-place upgrade	4.2 8.1 14.11
1.2	Given a scenario, use the appropriate Microsoft command-line tool. 1.2.1 - Navigation o 1.2.1.1 - cd o 1.2.1.2 - dir o 1.2.1.3 - md o 1.2.1.4 - rmdir o 1.2.1.5 - Drive navigation inputs o 1.2.1.5.1 - C:\ or D:\ or x:\	5.5, 5.8 7.1 8.1, 8.8 9.1 11.8, 11.9

		1.2.2 - Command-line tools
		  o 1.2.2.1 - ipconfig
		  o 1.2.2.2 - ping
		  o 1.2.2.3 - hostname
		  o 1.2.2.4 - netstat
		  o 1.2.2.5 - nslookup
		  o 1.2.2.6 - chkdsk
		  o 1.2.2.7 - net user
		  o 1.2.2.8 - net use
		  o 1.2.2.9 - tracert
		  o 1.2.2.10 - format
		  o 1.2.2.11 - xcopy
		  o 1.2.2.12 - copy
		  o 1.2.2.13 - robocopy
		  o 1.2.2.14 - gpupdate
		  o 1.2.2.15 - gpresult
		  o 1.2.2.16 - shutdown
		  o 1.2.2.17 - sfc
		  o 1.2.2.18 - [command name] /?
		  o 1.2.2.19 - diskpart
		  o 1.2.2.20 - pathping
		  o 1.2.2.21 - winver	

1.3	Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
	
	  1.3.1 - Task Manager
	    o 1.3.1.1 - Services
	    o 1.3.1.2 - Startup
	    o 1.3.1.3 - Performance
	    o 1.3.1.4 - Processes
	    o 1.3.1.5 - Users
	  1.3.2 - Microsoft Management Console (MMC) snap-in
	    o 1.3.2.1 - Event viewer (eventvwr.msc)
	    o 1.3.2.2 - Disk Management (diskmgmt.msc)
	    o 1.3.2.3 - Task Scheduler (taskschdd.msc)
	    o 1.3.2.4 - Device Manager (devmgmt.msc)
	    o 1.3.2.5 - Certificate Manager (certmgr.msc)
			5.5, 5.6, 5.7, 5.8, 5.9
			
			7.1, 7.3, 7.4
			
			8.1, 8.2
			
			10.4, 10.5
			
			14.11

	o 1.3.2.6 - Local Users and Groups (lusrmgr.msc)
	o 1.3.2.7 - Performance Monitor (perfmon.msc)
	o 1.3.2.8 - Group Policy Editor (gpedit.msc)
	1.3.3 - Additional tools
	     o 1.3.3.1 - System Information (msinfo32.exe)
	     o 1.3.3.2 - Resource Monitor (resmon.exe)
	     o 1.3.3.3 - System Configuration (msconfig.exe)
	     o 1.3.3.4 - Disk Cleanup (cleanmgr.exe)
	     o 1.3.3.5 - Disk Defragment (dfrgui.exe)
	     o 1.3.3.6 - Registry Editor (regedit.exe)	

1.4	Given a scenario, use the appropriate Microsoft Windows 10 Control Panel utility.
	
	1.4.1 - Internet Options
	1.4.2 - Devices and Printers
	1.4.3 - Programs and Features
	1.4.4 - Network and Sharing center
	1.4.5 - System
	1.4.6 - Windows Defender Firewall
	1.4.7 - Mail
	1.4.8 - Sound
	1.4.9 - User Accounts
	1.4.10 - Device Manager
	1.4.11 - Indexing Options
	1.4.12 - Administrative Tools
	1.4.13 - File Explorer Options
	     o 1.4.13.1 - Show hidden files
	     o 1.4.13.2 - Hide extensions
	     o 1.4.13.3 - General options
	     o 1.4.13.4 - View options
	1.4.14 - Power Options
	     o 1.4.14.1 - Hibernate
	     o 1.4.14.2 - Power plans
	     o 1.4.14.3 - Sleep/suspend
	     o 1.4.14.4 - Standby
	     o 1.4.14.5 - Choose what closing the lid does
	     o 1.4.14.6 - Turn on fast startup
		3.6, 3.7, 3.12
		7.1, 7.2
		
		9.1
		
		10.4, 10.5
		
		12.3
		
		14.8
		
		14.11

	o 1.4.14.7 - Universal Serial Bus (USB) selective suspend 1.4.15 - Ease of Access	
1.5	Given a scenario, use the appropriate Windows settings. 1.5.1 - Time and Language 1.5.2 - Update and Security 1.5.3 - Personalization 1.5.4 - Apps 1.5.5 - Privacy 1.5.6 - System 1.5.7 - Devices 1.5.8 - Network and Internet 1.5.9 - Gaming 1.5.10 - Accounts	7.2 8.2, 8.5 10.1
1.6	Given a scenario, configure Microsoft Windows networking features on a client/desktop. 1.6.1 - Workgroup vs. domain setup 　　o 1.6.1.1 - Shared resources 　　o 1.6.1.2 - Printers 　　o 1.6.1.3 - File servers 　　o 1.6.1.4 - Mapped drives 1.6.2 - Local OS firewall settings 　　o 1.6.2.1 - Application restrictions and exceptions 　　o 1.6.2.2 - Configuration 1.6.3 - Client network configuration 　　o 1.6.3.1 - Internet Protocol (IP) addressing scheme 　　o 1.6.3.2 - Domain Name System (DNS) settings 　　o 1.6.3.3 - Subnet mask 　　o 1.6.3.4 - Gateway 　　o 1.6.3.5 - Static vs. dynamic 1.6.4 - Establish network connections 　　o 1.6.4.1 - Virtual private network (VPN) 　　o 1.6.4.2 - Wireless	11.1, 11.3, 11.6, 11.7 12.5 14.8, 14.9 14.11

	o 1.6.4.3 - Wired o 1.6.4.4 - Wireless wide area network (WWAN) 1.6.5 - Proxy settings 1.6.6 - Public network vs. private network 1.6.7 - File Explorer navigation - network paths 1.6.8 - Metered connections and limitations	

1.7	Given a scenario, apply application installation and configuration concepts.
	
	    1.7.1 - System requirements for applications
	        o 1.7.1.1 - 32-bit vs. 64-bit dependent application requirements
	        o 1.7.1.2 - Dedicated graphics card vs. integrated
	        o 1.7.1.3 - Video random-access memory (VRAM) requirements
	        o 1.7.1.4 - RAM requirements
	        o 1.7.1.5 - Central processing unit (CPU) requirements
	        o 1.7.1.6 - External hardware tokens
	        o 1.7.1.7 - Storage requirements
	    1.7.2 - OS requirements for applications
	        o 1.7.2.1 - Application to OS compatibility
	        o 1.7.2.2 - 32-bit vs. 64-bit OS
	    1.7.3 - Distribution methods
	        o 1.7.3.1 - Physical media vs. downloadable
	        o 1.7.3.2 - ISO mountable
	    1.7.4 - Other considerations for new applications
	        o 1.7.4.1 - Impact to device
	        o 1.7.4.2 - Impact to network
	        o 1.7.4.3 - Impact to operation
	        o 1.7.4.4 - Impact to business
		3.5
		7.4

1.8	Explain common OS types and their purposes.
	
	    1.8.1 - Workstation OSs
	        o 1.8.1.1 - Windows
	        o 1.8.1.2 - Linux
	        o 1.8.1.3 - macOS
		4.1, 4.2, 4.3, 4.4
		5.5
		9.1, 9.4
		12.4

	o 1.8.1.4 - Chrome OS
	1.8.2 - Cell phone/tablet OSs
	       o 1.8.2.1 - iPadOS
	       o 1.8.2.2 - iOS
	       o 1.8.2.3 - Android
	1.8.3 - Various filesystem types
	       o 1.8.3.1 - New Technology File System (NTFS)
	       o 1.8.3.2 - File Allocation Table 32 (FAT32)
	       o 1.8.3.3 - Third extended filesystem (ext3)
	       o 1.8.3.4 - Fourth extended filesystem (ext4)
	       o 1.8.3.5 - Apple File System (APFS)
	       o 1.8.3.6 - Extensible File Allocation Table (exFAT)
	1.8.4 - Vendor life-cycle limitations
	       o 1.8.4.1 - End-of-life (EOL)
	       o 1.8.4.2 - Update limitations
	1.8.5 - Compatibility concerns between OSs	

1.9	Given a scenario, perform OS installations and upgrades in a diverse OS environment.
	
	1.9.1 - Boot methods
	       o 1.9.1.1 - USB
	       o 1.9.1.2 - Optical media
	       o 1.9.1.3 - Network
	       o 1.9.1.4 - Solid-state/flash drives
	       o 1.9.1.5 - Internet-based
	       o 1.9.1.6 - External/hot-swappable drive
	       o 1.9.1.7 - Internal hard drive (partition)
	1.9.2 - Types of installations
	       o 1.9.2.1 - Upgrade
	       o 1.9.2.2 - Recovery partition
	       o 1.9.2.3 - Clean install
	       o 1.9.2.4 - Image deployment
	       o 1.9.2.5 - Repair installation
	       o 1.9.2.6 - Remote network installation
	       o 1.9.2.7 - Other considerations
	       o 1.9.2.7.1 - Third-party drivers
	1.9.3 - Partitioning
		4.2
		5.5
		6.1, 6.2
		8.6
		10.4, 10.5

		o 1.9.3.1 - GUID [globally unique identifier] o 1.9.3.2 - Partition Table (GPT) o 1.9.3.3 - Master boot record (MBR) 1.9.4 - Drive format 1.9.5 - Upgrade considerations o 1.9.5.1 - Backup files and user preferences o 1.9.5.2 - Application and driver support/backward compatibility o 1.9.5.3 - Hardware compatibility 1.9.6 - Feature updates o 1.9.6.1 - Product life cycle	
1.10		Identify common features and tools of the macOS/desktop OS. 1.10.1 - Installation and uninstallation of applications o 1.10.1.1 - File types o 1.10.1.1.1 - .dmg o 1.10.1.1.2 - .pkg o 1.10.1.1.3 - .app o 1.10.1.2 - App Store o 1.10.1.3 - Uninstallation process 1.10.2 - Apple ID and corporate restrictions 1.10.3 - Best practices o 1.10.3.1 - Backups o 1.10.3.2 - Antivirus o 1.10.3.3 - Updates/patches 1.10.4 - System Preferences o 1.10.4.1 - Displays o 1.10.4.2 - Networks o 1.10.4.3 - Printers o 1.10.4.4 - Scanners o 1.10.4.5 - Privacy o 1.10.4.6 - Accessibility o 1.10.4.7 - Time Machine 1.10.5 - Features o 1.10.5.1 - Multiple desktops o 1.10.5.2 - Mission Control o 1.10.5.3 - Keychain	4.4 7.4 8.6 10.1, 10.2, 10.4 12.7

	o 1.10.5.4 - Spotlight o 1.10.5.5 - iCloud o 1.10.5.6 - Gestures o 1.10.5.7 - Finder o 1.10.5.8 - Remote Disc o 1.10.5.9 - Dock 1.10.6 - Disk Utility 1.10.7 - FileVault 1.10.8 - Terminal 1.10.9 - Force Quit	
1.11	Identify common features and tools of the Linux client/desktop OS. 1.11.1 - Common commands o 1.11.1.1 - ls o 1.11.1.2 - pwd o 1.11.1.3 - mv o 1.11.1.4 - cp o 1.11.1.5 - rm o 1.11.1.6 - chmod o 1.11.1.7 - chown o 1.11.1.8 - su/sudo o 1.11.1.9 - apt-get o 1.11.1.10 - yum o 1.11.1.11 - ip o 1.11.1.12 - df o 1.11.1.13 - grep o 1.11.1.14 - ps o 1.11.1.15 - man o 1.11.1.16 - top o 1.11.1.17 - find o 1.11.1.18 - dig o 1.11.1.19 - cat o 1.11.1.20 - nano 1.11.2 - Best practices o 1.11.2.1 - Backups o 1.11.2.2 - Antivirus	4.3 5.8 7.5 8.6 9.4 10.4 11.8 14.11

	o 1.11.2.3 - Updates/patches
	1.11.3 - Tools
	      o 1.11.3.1 - Shell/terminal
	      o 1.11.3.2 - Samba	

2.0	**Security**	

2.1	Summarize various security measures and their purposes.
	
	2.1.1 - Physical security
	      o 2.1.1.1 - Access control vestibule
	      o 2.1.1.2 - Badge reader
	      o 2.1.1.3 - Video surveillance
	      o 2.1.1.4 - Alarm systems
	      o 2.1.1.5 - Motion sensors
	      o 2.1.1.6 - Door locks
	      o 2.1.1.7 - Equipment locks
	      o 2.1.1.8 - Guards
	      o 2.1.1.9 - Bollards
	      o 2.1.1.10 - Fences
	2.1.2 - Physical security for staff
	      o 2.1.2.1 - Key fobs
	      o 2.1.2.2 - Smart cards
	      o 2.1.2.3 - Keys
	      o 2.1.2.4 - Biometrics
	      o 2.1.2.4.1 - Retina scanner
	      o 2.1.2.4.2 - Fingerprint scanner
	      o 2.1.2.4.3 - Palmprint scanner
	      o 2.1.2.5 - Lighting
	      o 2.1.2.6 - Magnetometers
	2.1.3 - Logical security
	      o 2.1.3.1 - Principle of least privilege
	      o 2.1.3.2 - Access control lists (ACLs)
	      o 2.1.3.3 - Multifactor authentication (MFA)
	      o 2.1.3.4 - Email
	      o 2.1.3.5 - Hard token
		8.1
		12.6
		
		14.1, 14.3, 14.4

	o 2.1.3.6 - Soft token
	      o 2.1.3.7 - Short message service (SMS)
	      o 2.1.3.8 - Voice call
	      o 2.1.3.9 - Authenticator application
	2.1.4 - Mobile device management (MDM)
	2.1.5 - Active Directory
	      o 2.1.5.1 - Login script
	      o 2.1.5.2 - Domain
	      o 2.1.5.3 - Group Policy/updates
	      o 2.1.5.4 - Organizational units
	      o 2.1.5.5 - Home folder
	      o 2.1.5.6 - Folder redirection
	      o 2.1.5.7 - Security groups	

2.2	Compare and contrast wireless security protocols and authentication methods.
	
	2.2.1 - Protocols and encryption
	      o 2.2.1.1 - WiFi Protected Access 2 (WPA2)
	      o 2.2.1.2 - WPA3
	      o 2.2.1.3 - Temporal Key Integrity Protocol (TKIP)
	      o 2.2.1.4 - Advanced Encryption Standard (AES)
	2.2.2 - Authentication
	      o 2.2.2.1 - Remote Authentication Dial-In User Service (RADIUS)
	      o 2.2.2.2 - Terminal Access Controller Access-Control System (TACACS+)
	      o 2.2.2.3 - Kerberos
	      o 2.2.2.4 - Multifactor
		9.3
		11.5
		
		12.6

2.3	Given a scenario, detect, remove, and prevent malware using the appropriate tools and methods.
	
	2.3.1 - Malware
	      o 2.3.1.1 - Trojan
	      o 2.3.1.2 - Rootkit
	      o 2.3.1.3 - Virus
	      o 2.3.1.4 - Spyware
	      o 2.3.1.5 - Ransomware
		8.7
		14.7, 14.8

	o 2.3.1.6 - Keylogger o 2.3.1.7 - Boot sector virus o 2.3.1.8 - Cryptominers 2.3.2 - Tools and methods o 2.3.2.1 - Recovery console o 2.3.2.2 - Antivirus o 2.3.2.3 - Anti-malware o 2.3.2.4 - Software firewalls o 2.3.2.5 - Anti-phishing training o 2.3.2.6 - User education regarding common threats o 2.3.2.7 - OS reinstallation		
2.4	Explain common social-engineering attacks, threats, and vulnerabilities. 2.4.1 - Social engineering o 2.4.1.1 - Phishing o 2.4.1.2 - Vishing o 2.4.1.3 - Shoulder Surfing o 2.4.1.4 - Whaling o 2.4.1.5 - Tailgating o 2.4.1.6 - Impersonation o 2.4.1.7 - Dumpster diving o 2.4.1.8 - Evil twin 2.4.2 - Threats o 2.4.2.1 - Distributed denial of service (DDoS) o 2.4.2.2 - Denial of service (DoS) o 2.4.2.3 - Zero-day attack o 2.4.2.4 - Spoofing o 2.4.2.5 - On-path attack o 2.4.2.6 - Brute-force attack o 2.4.2.7 - Dictionary attack o 2.4.2.8 - Insider threat o 2.4.2.9 - Structured Query Language (SQL) injection o 2.4.2.10 - Cross-site scripting (XSS) 2.4.3 - Vulnerabilities o 2.4.3.1 - Non-compliant systems o 2.4.3.2 - Unpatched systems	14.5	

	o 2.4.3.3 - Unprotected systems (missing antivirus/missing firewall) o 2.4.3.4 - EOL OSs o 2.4.3.5 Bring your own device (BYOD)	

2.5	Given a scenario, manage and configure basic security settings in the Microsoft Windows OS.
	
	2.5.1 - Defender Antivirus
	    o 2.5.1.1 - Activate/deactivate
	    o 2.5.1.2 - Updated definitions
	2.5.2 - Firewall
	    o 2.5.2.1 - Activate/deactivate
	    o 2.5.2.2 - Port security
	    o 2.5.2.3 - Application security
	2.5.3 - Users and groups
	    o 2.5.3.1 - Local vs. Microsoft account
	    o 2.5.3.2 - Standard account
	    o 2.5.3.3 - Administrator
	    o 2.5.3.4 - Guest user
	    o 2.5.3.5 - Power user
	2.5.4 - Login OS options
	    o 2.5.4.1 - Username and password
	    o 2.5.4.2 - Personal identification number (PIN)
	    o 2.5.4.3 - Fingerprint
	    o 2.5.4.4 - Facial recognition
	    o 2.5.4.5 - Single sign-on (SSO)
	2.5.5 - NTFS vs. share permissions
	    o 2.5.5.1 - File and folder attributes
	    o 2.5.5.2 - Inheritance
	2.5.6 - Run administrator vs. standard user
	    o 2.5.6.1 - User Account Control (UAC)
	2.5.7 - Bitlocker
	2.5.8 - Bitlocker To Go
	2.5.9 - Encrypting File System (EFS)
		8.2
		9.1, 9.2, 9.3
		
		14.1, 14.7, 14.8

2.6	Given a scenario, configure a workstation to meet best practices for security.	9.3

	2.6.1 - Data-at-rest encryption
	2.6.2 - Password best practices
	  o 2.6.2.1 - Complexity requirements
	  o 2.6.2.1.1 - Length
	  o 2.6.2.1.2 - Character types
	  o 2.6.2.2 - Expiration requirements
	  o 2.6.2.3 - Basic input/output system (BIOS)/Unified Extensible Firmware Interface (UEFI) passwords
	2.6.3 - End-user best practices
	  o 2.6.3.1 - Use screensaver locks
	  o 2.6.3.2 - Log off when not in use
	  o 2.6.3.3 - Secure/protect critical hardware (e.g., laptops)
	  o 2.6.3.4 - Secure personally identifiable information (PII) and passwords
	2.6.4 - Account management
	  o 2.6.4.1 - Restrict user permissions
	  o 2.6.4.2 - Restrict login times
	  o 2.6.4.3 - Disable guest account
	  o 2.6.4.4 - Use failed attempts lockout
	  o 2.6.4.5 - Use timeout/screen lock
	2.6.5 - Change default administrator's user account/password
	2.6.6 - Disable AutoRun
	2.6.7 - Disable AutoPlay
			14.1
			
			14.11

2.7	Explain common methods for securing mobile and embedded devices.
	
	2.7.1 - Screen locks
	  o 2.7.1.1 - Facial recognition
	  o 2.7.1.2 - PIN codes
	  o 2.7.1.3 - Fingerprint
	  o 2.7.1.4 - Pattern
	  o 2.7.1.5 - Swipe
	2.7.2 - Remote wipes
	2.7.3 - Locator applications
	2.7.4 - OS updates
	2.7.5 - Device encryption
	2.7.6 - Remote backup applications
			12.6

	2.7.7 - Failed login attempts restrictions
	2.7.8 - Antivirus/anti-malware
	2.7.9 - Firewalls
	2.7.10 - Policies and procedures
	    o 2.7.10.1 - BYOD vs. corporate owned
	    o 2.7.10.2 - Profile security requirements
	2.7.11 - Internet of Things (IoT)	

2.8	Given a scenario, use common data destruction and disposal methods.
	
	2.8.1 - Physical destruction
	    o 2.8.1.1 - Drilling
	    o 2.8.1.2 - Shredding
	    o 2.8.1.3 - Degaussing
	    o 2.8.1.4 - Incinerating
	2.8.2 - Recycling or repurposing best practices
	    o 2.8.2.1 - Erasing/wiping
	    o 2.8.2.2 - Low-level formatting
	    o 2.8.2.3 - Standard formatting
	2.8.3 - Outsourcing concepts
	    o 2.8.3.1 - Third-party vendor
	    o 2.8.3.2 - Certification of destruction/recycling
		14.6

2.9	Given a scenario, configure appropriate security settings on small office/home office (SOHO) wireless and wired networks.
	
	2.9.1 - Home router settings
	    o 2.9.1.1 - Change default passwords
	    o 2.9.1.2 - IP filtering
	    o 2.9.1.3 - Firmware updates
	    o 2.9.1.4 - Content filtering
	    o 2.9.1.5 - Physical placement/secure locations
	    o 2.9.1.6 - Dynamic Host Configuration Protocol (DHCP) reservations
	    o 2.9.1.7 - Static wide-area network (WAN) IP
	    o 2.9.1.8 - Universal Plug and Play (UPnP)
		11.6
		14.11

	○ 2.9.1.9 - Screened subnet
	   2.9.2 - Wireless specific
	    ○ 2.9.2.1 - Changing the service set identifier (SSID)
	    ○ 2.9.2.2 - Disabling SSID broadcast
	    ○ 2.9.2.3 - Encryption settings
	    ○ 2.9.2.4 - Disabling guest access
	    ○ 2.9.2.5 - Changing channels
	   2.9.3 - Firewall settings
	    ○ 2.9.3.1 - Disabling unused ports
	    ○ 2.9.3.2 - Port forwarding/mapping	

2.10	Given a scenario, install and configure browsers and relevant security settings.
	
	   2.10.1 - Browser download/installation
	    ○ 2.10.1.1 - Trusted sources
	    ○ 2.10.1.1.1 - Hashing
	    ○ 2.10.1.2 - Untrusted sources
	   2.10.2 - Extensions and plug-ins
	    ○ 2.10.2.1 - Trusted sources
	    ○ 2.10.2.2 - Untrusted sources
	   2.10.3 - Passwords managers
	   2.10.4 - Secure connections/sites - valid certificates
	   2.10.5 - Settings
	    ○ 2.10.5.1 - Pop-up blocker
	    ○ 2.10.5.2 - Clearing browsing data
	    ○ 2.10.5.3 - Clearing cache
	    ○ 2.10.5.4 - Private-browsing mode
	    ○ 2.10.5.5 - Sign-in/browser data synchronization
	    ○ 2.10.5.6 - Ad blockers
		14.10

3.0	**Software Troubleshooting**	
3.1	Given a scenario, troubleshoot common Windows OS problems. 3.1.1 - Common symptoms	4.2 5.8

		o 3.1.1.1 - Blue screen of death (BSOD)
		o 3.1.1.2 - Sluggish performance
		o 3.1.1.3 - Boot problems
		o 3.1.1.4 - Frequent shutdowns
		o 3.1.1.5 - Services not starting
		o 3.1.1.6 - Applications crashing
		o 3.1.1.7 - Low memory warnings
		o 3.1.1.8 - USB controller resource warnings
		o 3.1.1.9 - System instability
		o 3.1.1.10 - No OS found
		o 3.1.1.11 - Slow profile load
		o 3.1.1.12 - Time drift
		3.1.2 - Common troubleshooting steps
		    o 3.1.2.1 - Reboot
		    o 3.1.2.2 - Restart services
		    o 3.1.2.3 - Uninstall/reinstall/update applications
		    o 3.1.2.4 - Add resources
		    o 3.1.2.5 - Verify requirements
		    o 3.1.2.6 - System file check
		    o 3.1.2.7 - Repair Windows
		    o 3.1.2.8 - Restore
		    o 3.1.2.9 - Reimage
		    o 3.1.2.10 - Roll back updates
		    o 3.1.2.11 - Rebuild Windows profiles
			7.8
			
			8.7, 8.8
			
			10.5

3.2		Given a scenario, troubleshoot common personal computer (PC) security issues.
		
		3.2.1 - Common symptoms
		    o 3.2.1.1 - Unable to access the network
		    o 3.2.1.2 - Desktop alerts
		    o 3.2.1.3 - False alerts regarding antivirus protection
		    o 3.2.1.4 - Altered system or personal files
		    o 3.2.1.5 - Unwanted notifications within the OS
		    o 3.2.1.6 - OS update failures
		3.2.2 - Browser-related symptoms
		    o 3.2.2.1 Random/frequent pop-ups
		    o 3.2.2.2 Certificate warnings
			3.8
			8.5
			
			14.11

	o 3.2.2.3 Redirection	

3.3	Given a scenario, use best practice procedures for malware removal.
	
	3.3.1 - Investigate and verify malware symptoms
	3.3.2 - Quarantine infected systems
	3.3.3 - Disable System Restore in Windows
	3.3.4 - Remediate infected systems
	     o 3.3.4.1 - Update anti-malware software
	     o 3.3.4.2 - Scanning and removal techniques (e.g., safe mode, preinstallation environment)
	3.3.5 - Schedule scans and run updates
	3.3.6 - Enable System Restore and create a restore point in Windows
	3.3.7 - Educate the end user
		14.7

3.4	Given a scenario, troubleshoot common mobile OS and application issues.
	
	3.4.1 - Common symptoms
	     o 3.4.1.1 - Application fails to launch
	     o 3.4.1.2 - Application fails to close/crashes
	     o 3.4.1.3 - Application fails to update
	     o 3.4.1.4 - Slow to respond
	     o 3.4.1.5 - OS fails to update
	     o 3.4.1.6 - Battery life issues
	     o 3.4.1.7 - Randomly reboots
	     o 3.4.1.8 - Connectivity issues
	     o 3.4.1.9 - Screen does not autorotate
		12.3

3.5	Given a scenario, troubleshoot common mobile OS and application security issues.
	
	3.5.1 - Security concerns
	     o 3.5.1.1 - Android package (APK) source
	     o 3.5.1.2 - Developer mode
	     o 3.5.1.3 - Root access/jailbreak
		14.11

		o 3.5.1.4 - Bootleg/malicious application	
		3.5.2 - Common symptoms	
		o 3.5.2.1 - High network traffic	
		o 3.5.2.2 - Sluggish response time	
		o 3.5.2.3 - Data-usage limit notification	
		o 3.5.2.4 - Limited Internet connectivity	
		o 3.5.2.5 - No Internet connectivity	
		o 3.5.2.6 - High number of ads	
		o 3.5.2.7 - Fake security warnings	
		o 3.5.2.8 - Unexpected application behavior	
		o 3.5.2.9 - Leaked personal files/data	
4.0	**Operational Procedures**		

4.1	Given a scenario, implement best practices associated with documentation and support systems information management.
	
	    4.1.1 - Ticketing systems
	       o 4.1.1.1 - User information
	       o 4.1.1.2 - Device information
	       o 4.1.1.3 - Description of problems
	       o 4.1.1.4 - Categories
	       o 4.1.1.5 - Severity
	       o 4.1.1.6 - Escalation levels
	       o 4.1.1.7 - Clear, concise written communication
	       o 4.1.1.7.1 - Problem description
	       o 4.1.1.7.2 - Progress notes
	       o 4.1.1.7.3 Problem resolution
	    4.1.2 - Asset management
	       o 4.1.2.1 - Inventory lists
	       o 4.1.2.2 - Database system
	       o 4.1.2.3 - Asset tags and IDs
	       o 4.1.2.4 - Procurement life cycle
	       o 4.1.2.5 - Warranty and licensing
	       o 4.1.2.6 - Assigned users
	    4.1.3 - Types of documents
		2.8, 2.9
		3.4
		
		5.5
		
		6.2
		
		11.9	

		o 4.1.3.1 - Acceptable use policy (AUP) o 4.1.3.2 - Network topology diagram o 4.1.3.3 - Regulatory compliance requirements o 4.1.3.3.1 - Splash screens o 4.1.3.4 - Incident reports o 4.1.3.5 - Standard operating procedures o 4.1.3.5.1 - Procedures for custom installation of software package o 4.1.3.6 - New-user setup checklist o 4.1.3.7 - End-user termination checklist 4.1.4 - Knowledge base/articles	
4.2	Explain basic change-management best practices. 4.2.1 - Documented business processes o 4.2.1.1 - Rollback plan o 4.2.1.2 - Sandbox testing o 4.2.1.3 - Responsible staff member 4.2.2 - Change management o 4.2.2.1 - Request forms o 4.2.2.2 - Purpose of the change o 4.2.2.3 - Scope of the change o 4.2.2.4 - Date and time of the change o 4.2.2.5 - Affected systems.impact o 4.2.2.6 - Risk analysis o 4.2.2.6.1 - Risk level o 4.2.2.7 - Change board approvals o 4.2.2.8 - End-user acceptance	2.4	
4.3	Given a scenario, implement workstation backup and recovery methods. 4.3.1 - Backup and recovery o 4.3.1.1 - Full o 4.3.1.2 - Incremental o 4.3.1.3 - Differential o 4.3.1.4 - Synthetic	8.6	

	4.3.2 - Backup testing
	     o 4.3.2.1 - Frequency
	4.3.3 - Backup rotation schemes
	     o 4.3.3.1 - On site vs. off site
	     o 4.3.3.2 - Grandfather-father-son (GFS)
	     o 4.3.3.3 - 3-2-1 backup rule	

4.4	Given a scenario, use common safety procedures.
	
	4.4.1 - Electrostatic discharge (ESD) straps
	4.4.2 - ESD mats
	4.4.3 - Equipment grounding
	4.4.4 - Proper power handling
	4.4.5 - Proper component handling and storage
	4.4.6 - Antistatic bags
	4.4.7 - Compliance with government regulations
	4.4.8 - Personal safety
	     o 4.4.8.1 - Disconnect power before repairing PC
	     o 4.4.8.2 - Lifting techniques
	     o 4.4.8.3 - Electrical fire safety
	     o 4.4.8.4 - Safety goggles
	     o 4.4.8.5 - Air filtration mask
		2.1, 2.6
		3.6

4.5	Summarize environmental impacts and local environmental controls.
	
	4.5.1 - Material safety data sheet (MSDS)/documentation for handling and disposal
	     o 4.5.1.1 - Proper battery disposal
	     o 4.5.1.2 - Proper toner disposal
	     o 4.5.1.3 - Proper disposal of other devices and assets
	4.5.2 - Temperature, humidity-level awareness, and proper ventilation
	     o 4.5.2.1 - Location/equipments placement
	     o 4.5.2.2 - Dust cleanup
	     o 4.5.2.3 - Compressed air/vacuums
	4.5.3 - Power surges, brownouts, and blackouts
	     o 4.5.3.1 - Battery backup
		1.1
		2.1, 2.2, 2.5
		
		13.1

	o 4.5.3.2 - Surge supressor	

4.6	Explain the importance of prohibited content/activity and privacy, licensing, and policy concepts.
	
	4.6.1 - Incident response
	    o 4.6.1.1 - Chain of custody
	    o 4.6.1.2 - Inform management/law enforcement as necessary
	    o 4.6.1.3 - Copy of drive (data integrity and preservation)
	    o 4.6.1.4 - Documentation of incident
	4.6.2 - Licensing/digital rights management (DRM)/end-user license agreement (EULA)
	    o 4.6.2.1 - Valid licenses
	    o 4.6.2.2 - Non-expired licenses
	    o 4.6.2.3 - Personal use license vs. corporate use license
	    o 4.6.2.4 - Open-source license
	4.6.3 - Regulated data
	    o 4.6.3.1 - Credit card transactions
	    o 4.6.3.2 - Personal government-issued information
	    o 4.6.3.3 - PII
	    o 4.6.3.4 - Healthcare data
	    o 4.6.3.5 - Data retention requirements
		7.6
		14.2

4.7	Given a scenario, use proper communication techniques and professionalism.
	
	4.7.1 - Professional appearance and attire
	    o 4.7.1.1 - Match the required attire of the given environment
	    o 4.7.1.1.1 - Formal
	    o 4.7.1.1.2 - Business casual
	4.7.2 - Use proper language and avoid jargon, acronyms, and slang, when applicable
	4.7.3 - Maintain a positive attitude/project confidence
	4.7.4 - Actively listen, take notes, and avoid interrupting the customer
	4.7.5 - Be culturally sensitive
	    o 4.7.5.1 - Use appropriate professional titles, when applicable
	4.7.6 - Be on time (if late, contact the customer)
	4.7.7 - Avoid distractions
	    o 4.7.7.1 - Personal calls
		2.3

	o　4.7.7.2 - Texting/social media sites o　4.7.7.3 - Personal interruptions 4.7.8 - Dealing with difficult customers or situations 　　　o　4.7.8.1 - Do not argue with customers or be defensive 　　　o　4.7.8.2 - Avoid dismissing customer problems 　　　o　4.7.8.3 - Avoid being judgmental 　　　o　4.7.8.4 - Clarify customer statements (ask open-ended questions to narrow the scope of the problem, restate the issue, or question to verify understanding) 　　　o　4.7.8.5 - Do not disclose experience via social media outlets 4.7.9 - Set and meet expectations/timeline and communicate status with the customer 　　　o　4.7.9.1 - Offer repair/replacement options, as needed 　　　o　4.7.9.2 - Provide proper documentation on the services provided 　　　o　4.7.9.3 - Follow up with customer/user at a later date to verify satisfaction 4.7.10 - Deal appropriately with customers' confidential and private materials 　　　o　4.7.10.1 - Located on a computer, desktop, printer, etc.	
4.8	Identify the basics of scripting. 4.8.1 - Script file types 　　　o　4.8.1.1 - .bat 　　　o　4.8.1.2 - .ps1 　　　o　4.8.1.3 - .vbs 　　　o　4.8.1.4 - .sh 　　　o　4.8.1.5 - .js 　　　o　4.8.1.6 - .py 4.8.2 - Use cases for scripting 　　　o　4.8.2.1 - Basic automation 　　　o　4.8.2.2 - Restarting machines 　　　o　4.8.2.3 - Remapping network drives 　　　o　4.8.2.4 - Installation of applications 　　　o　4.8.2.5 - Automated backups 　　　o　4.8.2.6 - Gathering of information/data 　　　o　4.8.2.7 - Initiating updates 4.8.3 - Other considerations when using scripts 　　　o　4.8.3.1 - Unintentionally introducing malware 　　　o　4.8.3.2 - Inadvertently changing system settings	7.9

	o 4.8.3.3 - Browser or system crashes due to mishandling of resources	

4.9	Given a scenario, use remote access technologies.
	
	        4.9.1 - Methods/tools
	                o 4.9.1.1 - RDP
	                o 4.9.1.2 - VPN
	                o 4.9.1.3 - Virtual network computer (VNC)
	                o 4.9.1.4 - Secure Shell (SSH)
	                o 4.9.1.5 - Remote monitoring and management (RMM)
	                o 4.9.1.6 - Microsoft Remote Assistance (MSRA)
	                o 4.9.1.7 - Third-party tools
	                o 4.9.1.7.1 - Screen-sharing software
	                o 4.9.1.7.2 - Video-conferencing software
	                o 4.9.1.7.3 - File transfer software
	                o 4.9.1.7.4 - Desktop management software
	        4.9.2 - Security considerations of each access method
		7.1
		8.3, 8.4