1.1 Compare and contrast notational systems.

Binary	Data type support 1-bit storage, representing FALSE and TRUE
	Boolean logic is a statement that resolves to a true or false condition and underpins the branching and looping features of computer code.
Hexade-cimal	Notational system with 16 values per digit. Values above 9 are represented by the letters A,B,C,D,E,F.
	Hex is a compact way of referring to long byte values, such as MAC and IPv6 addresses.
Float	Data type supporting storage of floating point numbers (decimal fractions).
ASCII	7-bit code page mapping binary values to character glyphs
	Standard ASCII can represent 127 characters, though some values are reserved for non-printing control characters.
Unicode	Extensible system of code pages capable of representing millions of character glyphs, allowing for international alphabets.

1.2 Data types and their characteristics

Char	Data type supporting storage of a single character.
String	Data type supporting storage of a variable length series of characters.
Integer	Data type supporting storage of whole numbers.
Float	Data type supporting storage of floating point numbers (decimal fractions).
Boolean	Data type support 1-bit storage, representing FALSE and TRUE
	Boolean logic is a statement that resolves to a true or false condition and underpins the branching and looping features of computer code.

1.3 Basics of computing and processing.

Input	the computer receives data entered by the user through peripheral devices, such as mice, keyboards, scanners, cameras, and microphones.
Processing	the data is written to memory and manipulated by the CPU, acting on instructions from the operating system and applications software.
Output	the processed data is shown or played to the user through an output device, such as a monitor or loudspeaker system.
Storage	the data may be written to different types of storage devices, such as hard disks or optical discs, because data stored in most types of system memory is only preserved while the computer is powered on.

Additionally, most computers are configured in networks, allowing them to exchange data. You can think of networking as a special class of input and output, but it is probably more helpful to conceive of it as a separate function.

1.4 Vallue of data and information

Data and information as assets	For organisations, computer data can be considered an asset
	An asset is something of commercial value

1.4 Vallue of data and information (cont)		
Investing in security	A mechanism designed to protect an information asset or processing system is called a security control	
	they are designed to prevent, deter, detect, and/or recover from attempts to view or modify data without authorization.	
	can be costly, both in terms of purchasing hardware and software and in terms of more complex procedures and staff training.	
Return on Security Investment (ROSI)	This is the calculation made for the case of investing in security.	
	This is done by performing **risk assessments** to work out how much the loss of data would cost and how likely it is that data loss might occur.	
	The use of security controls should reuce the impact and likelihood of losses, justifying the investment made	
Security Controls		
Backup	ensure that you maintain copies of your data and that these copies can be quickly and easily accessed when necessary.	
Access control	The control of access to stored data via:	
	Permissions	assign permissions on data files to users and groups of users.
	Usage restrictions	use rights management software to control what users can do with data files
	Data encryption	data is encoded in some way that only a person with the correct key can read it

1.5 Common units of measure.	
Data storage Units	The fundamental unit of data storage is the bit (binary digit) which can represent 1 or 0

1.5 Common units of measure. (cont)		
	Bit	basic unit of computer data
		can represent two values (zero or one)
	Byte	8 bits
		The first multiple of bits
	Double byte	16 bits
	KiloByte (KB)	1000 bytes
		(or 103 or 10*10*10 bytes)
		Small files are often measured in KB.
	MegaByte (MB)	1000 KB
		1000*1000 bytes
		(or 1,000,000 bytes)
		Many files would be measured in megabytes.
	GigaByte (GB)	1000 MB
		1000*1000*1000 bytes
		(1,000,000,000 bytes)
		Gigabytes are usually used to talk about disk capacity.
	TeraByte (TB)	1000 GB
		(1,000,000,000,000 bytes)
		ome individual disk units might be 1 or 2 terabytes but these units are usually used to describe large storage networks.
	PetaByte (PB)	1000 TB
		or 1015 bytes (1,000,000,000,000,000 bytes)
		The largest storage networks and cloud systems would have petabytes of capacity.
Throughput Rate Units/Transfer Rate	rate that a particular connection can sustain is measured in bits per second (bps)	
	The amount of data that can be transferred over a network connection in a given amount of time, typically measured in bits or bytes per second (or some more suitable multiple thereof).	

1.5 Common units of measure. (cont)

	described variously as data rate, bit rate, connection speed, transmission speed, or (sometimes inaccurately) bandwidth or baud	
	often quoted as the peak, maximum, theoretical value; sustained, actual throughput is often considerably less.	
	Kbps (or Kb/s)	1000 bits per second
		Older computer peripheral interfaces (or buses) and slow network links would be measured in Kbps.
	Mbps (or Mb/s)	1000Kbps
		1,000,000 bits per second.
		Many internal computer interfaces have throughputs measured in Mbps
		Wireless networks and residential Internet links also typically have this sort of throughput.
	Gbps (or Gb/s)	1000Mpbs
		1,000,000,000 bits per second
		The latest PC bus standards and networks can support this higher level of throughput.
	Tbps (or Tb/s)	1000Gbps
		1,000,000,000,000 bits per second
		This sort of capacity is found in major telecommunications links between data centers, cities, and countries.
Throughput units are **always** base 10.		
Processing Speed Units	A computer's internal clock and the speed at which its processors work is measured in units of time called Hertz (Hz). 1 Hz represents one cycle per second.	
	Megahertz (MHz)	1 million (1,000,000) cycles per second.
		Older PC bus interfaces and many types of network interfaces work at this slower signaling speed.

1.5 Common units of measure. (cont)

Gigahertz (GHz)	1000 million (1,000,000,000) cycles per second.
	Modern CPUs and bus types plus fiber-optic network equipment work at these much faster speeds.

1.6 Explain the troubleshooting methodology.

Troubleshooting is a process of problem solving. It is important to realize that problems have causes, symptoms, and consequences. For example:

CompTIA Troubleshooting Model

1. **Identify** the problem:	Gather information.
	Duplicate the problem(observe as it occurs. via remote desktop, lab system or VM)
	Question users (how, when, who, changes)
	Identify symptoms.
	Determine if anything has changed.
	Approach multiple problems individually. - if problems related, treat each as a separate case. if related, check for outstanding support or maintenance tickets.)
2. **Research** knowledge base/Internet	observe in operation via remote desktop or in-person
	View system, application, or network log files.
	Monitor other support requests to identify similar problems
Understanding the Problem	determine a theory of probable cause from analysis of the symptoms
3. Establish a theory of **probable cause**	Question the obvious.
	Step through the process of using the system or application making sure that you verify even the simplest steps by questioning the obvious
	Consider multiple approaches.

1.6 Explain the troubleshooting methodology. (cont)		
	Divide and conquer(Using tests to helps you more quickly identify probable causes.)	
	Workarounds (provides a way for the user to continue to work with the system)	
4. **Test** the theory to determine cause.	Once the theory is confirmed (confirmed root cause), determine the next steps to resolve the problem.	
	If the theory is not confirmed, establish a new theory or escalate.	
	establish a root cause for the problem	
5. Establish a **plan of action** to resolve the problem and identify potential effects.	establish a plan of action to eliminate the root cause without destabilizing some other part of the system.	
	Repair	you need to determine whether the cost of repair/time taken to reconfigure something makes this the best option.
	Replace	often more expensive and may be time-consuming if a part is not available. There may also be an opportunity to upgrade the device or software.
	Ignore	as any software developer will tell you, not all problems are critical. If neither repair nor replace is cost-effective, it may be best either to find a workaround or just to document the issue and move on.
6.**Implement** the solution or escalate as necessary.	Your plan of action should contain the detailed steps and resources required to implement the solution. As well as these practical steps, you have to consider the issue of authorization	

1.6 Explain the troubleshooting methodology. (cont)	
	If applying the solution is disruptive to the wider network, you also need to consider the most appropriate time to schedule the reconfiguration work and plan how to notify other network users.
7. **Verify** full system functionality and, if applicable, implement preventive measures.	identify the results and effects of the solution
	Ensure that you were right and that the problem is resolved
	Restate what the problem was and how it was resolved then confirm with the customer that the incident log can be closed.
	To fully solve the root cause of a problem, you should try to eliminate any factors that may cause the problem to recur.
6. **Document** findings/lessons learned, actions and outcomes.	it is important that information about the problem, tests performed, and attempted resolutions are recorded
	when a problem is resolved, a complete record exists documenting the symptoms, possible causes investigated, and the ultimate resolution

2.1 types of input/output device interfaces		
Networking		
Wired		
RJ (Registered Jack) Connector	Ethernet Connector	used for twisted pair cabling. 4-pair network cabling uses the larger **RJ-45** connector.
	Modem/telephone	2=pair cabling uses the RJ-11 connector.
Wireless		

2.1 types of input/output device interfaces (cont)

Bluetooth	Short-range radio-based technology, working at up to 10m (30 feet) at up to 1 Mbps used to connect peripherals (such as mice, keyboards, and printers) and for communication between two devices (such as a laptop and smartphone).
	The advantage of radio-based signals is that devices do not need line-of-sight, though the signals can still be blocked by thick walls and metal and can suffer from interference from other radio sources operating at the same frequency (2.4 GHz)
	Bluetooth Low Energy (BLE) is designed for small battery-powered devices that transmit small amounts of data infrequently
	BLE is not backwards-compatible with "classic" Bluetooth though a device can support both standards simultaneously.
RFID (Radio Frequency Identification)	A chip allowing data to be read wirelessly.
NFC (Nearfield Communications)	Standard for peer-to-peer (2-way) radio communications over very short (around 4") distances, facilitating contactless payment and similar technologies.
	NFC is based on RFID.

Peripheral devices

By **Bayan** (Bayan.A)
cheatography.com/bayan-a/

Published 15th December, 2022.
Last updated 9th December, 2022.

2.1 types of input/output device interfaces (cont)		
USB (Universal Serial Bus)	USB permits the connection of up to 127 different peripherals. A larger Type A connector attaches to a port on the host; Type B and Mini- or Micro- Type B connectors are used for devices.	
	USB 1.1 supports 12 Mbps while USB 2.0 supports 480 Mbps and is backward compatible with 1.1 devices (which run at the slower speed).	
	USB devices are hot swappable.	(Hot swappable: a device that can be added or removed without having to restart the operating system)
	A device can draw up to 2.5W power.	
	USB 3.0 defines a 4.8 Gbps SuperSpeed rate and can deliver 4.5W power.	
Firewire (IEEE 1394 Standard)	This serial SCSI bus standard supports high data rates (up to 400 Mbps) and this in turn, makes it attractive for applications requiring intensive data transfer (such as video cameras, satellite receivers, and digital media players).	
	Firewire is the brand name for the IEEE standard 1394.	
Thunderbolt	interface was developed by Intel and is primarily used on Apple workstations and laptops.	
	can be used as a display interface (like DisplayPort) and as a general peripheral interface (like USB 3).	
Graphic Devices		
VGA (Video Graphics Array) Connector	A 15-pin HD connector has been used to connect the graphics adapter to a monitor since 1987.	

2.1 types of input/output device interfaces (cont)	
HDMI (High Definition Multimedia Interface)	High-specification digital connector for audio-video equipment.
Digital Visual Interface (DVI)	high-quality digital interface designed for flat-panel display equipment.
	Single- or dual-link—dual-link makes more bandwidth available. This may be required for resolutions better than HDTV (1920x1200).
	Analog and/or digital—DVI-I supports analog equipment (such as CRTs) and digital. DVI-A supports only analog equipment, and DVI-D supports only digital.
	DVI has been superseded by HDMI and DisplayPort/Thunderbolt but was very widely used on graphics adapters and computer displays.
DisplayPort	royalty-free standard intended to "complement" HDMI.
	uses a 20-pin connector.
	A DP++ port allows a connection with DVI-D and HDMI devices (using a suitable adapter cable)
mini DisplayPort format (MiniDP or mDP)	developed by Apple and licensed to other vendors.
	uses the same physical interface as Thunderbolt

2.2 Set up peripherals	
Plug-and-Play (PnP)	A Plug-and-Play system (comprising a compatible BIOS, operating system, and hardware) is self-configuring.
Mouse	A mouse can be interfaced using a PS/2, USB, or wireless (IrDA or Bluetooth) port.
	Optical mouse—this uses LEDs to detect movement over a surface.
	Laser mouse—this uses an infrared laser, which gives greater precision than an optical mouse.

2.2 Set up peripherals (cont)	
	essential device to implement a WIMP GUI, a mouse simply controls the movement of a cursor that can be used to select objects from the screen.
	also feature a scroll wheel.
	All Windows mice feature two click buttons, which are configured to perform different actions.
	A standard mouse does not need a special driver installing and basic settings can be configured using the Mouse applet in Control Panel/Settings
	many different designs and layouts for different countries. Some keyboards feature special keys.
Keyboard	Desktop keyboards can have PS/2, USB, or wireless (IrDA or Bluetooth) interfaces
	to access and configure extra buttons on some mice you will need to install the manufacturer's driver.
	When a hardware device is added or removed, the operating system detects the change and automatically installs the appropriate drivers
	use the Keyboard applet in Control Panel to configure it.
Keyboard Regionalization	can vary from country to country
	type of keyboard layout is configured through the Language applet in Control Panel/Setting
	key combo (START+SPACEBAR in Windows 10) can be used to switch between the different layouts(if enabled)

2.3 Internal computing components	
Motherboard	provides the basic foundation for all of the computer's hardware including the processor, RAM, BIOS, and expansion cards.
BIOS (Basic Input/Output System)	The BIOS is firmware that contains programs and information relating to the basic operation of PC components such as drives, keyboard, video display, and ports.
	It also contains specific routines to allow set-up configuration to be viewed and edited and it contains the self-diagnostic Power-On Self-Test (POST) program used to detect fundamental faults in PC components
	BIOS can also be used to secure components not protected by the OS by specifying a supervisor password (to prevent tampering with BIOS settings) and a user password (to boot the PC).
RAM (Random Access Memory)	Random Access Memory is the principal storage space for computer data and program instructions

2.3 Internal computing components (cont)	
	RAM is generally described as being volatile in the sense that once power has been removed or the computer has been rebooted, data is lost.
ARM (Advanced RISC Machines)	Designer of CPU and chipset architectures widely used in mobile devices.
	RISC stands for Reduced Instruction Set Computing.
	RISC microarchitectures use simple instructions processed very quickly
	This contrasts with Complex (CISC) microarchitectures, which use more powerful instructions but process each one more slowly.
32-bit versus 64-bit	Processing modes referring to the size of each instruction processed by the CPU. 32-bit CPUs replaced earlier 16-bit CPUs and were used through the 1990s to the present day, though most CPUs now work in 64-bit mode.
	The main 64-bit platform is called AMD64 or EM64T (by Intel)
	This platform is supported by 64-bit versions of Windows as well as various Linux distributions
	Software can be compiled as 32-bit or 64-bit. 64-bit CPUs can run most 32-bit software but a 32-bit CPU cannot execute 64-bit software.
HDD (Hard Disk Drive)	High capacity units typically providing persistent mass storage for a PC (saving data when the computer is turned off).
	Data is stored using platters with a magnetic coating that are spun under disk heads that can read and write to locations on each platter (sectors)
	A HDD installed within a PC is referred to as the fixed disksA HDD installed within a PC is referred to as the fixed disks
	HDDs are often used with enclosures as portable storage or as Network Attached Storage (NAS).HDDs are often used with enclosures as portable storage or as Network Attached Storage (NAS).
SD (Secure Digital) CardSD (Secure Digital) Card	One of the first types of flash memory card.
Solid State Drive (SSD)	use a type of transistor-based memory called flash memory and are much faster than HDDs.

2.3 Internal computing components (cont)	
Cooling Device	A CPU generates a large amount of heat that must be dissipated to prevent damage to the chip
	Generally, a CPU will be fitted with a heatsink (a metal block with fins) and fan
	Thermal compound is used at the contact point between the chip and the heatsink to ensure good heat transfer.
	The PSU also incorporates a fan to expel warm air from the system.
	Modern motherboards have temperature sensors that provide warning of overheating before damage can occur.
	Very high performance or overclocked systems or systems designed for quiet operation may require more sophisticated cooling systems, such as liquid cooling.
	Cooling systems that work without electricity are described as passive; those requiring a power source are classed as active.
Liquid Cooling System	Using water piped around the PC and heatsinks for cooling.
	This is more efficient and allows for fewer fans and less noise.
Graphics Processing Unit (GPU)	display functions are often performed by a dedicated processor
	Displays high-resolution images that requires a lot of processing power, especially if the image changes rapidly, as with video, or uses complicated 3D and texture effects, as with computer games.
Video Card	Provides the interface between the graphics components of the computer and the display device.
	A number of connectors may be provided for the display, including VGA, DVI, and HDMI.
	Graphics adapters receive information from the microprocessor and store this data in video RAM.
	An adapter may support both analog and digital outputs or analog/digital only (as most LCDs use digital inputs the use of analog outputs is declining).
	Most adapters come with their own processor (Graphics Processing Unit [GPU]) and onboard memory.

2.3 Internal computing components (cont)	
Network Adapter (NIC [Network Interface Card])	The network adapter allows a physical connection between the host and the transmission media
	A NIC can address other cards and can recognize data that is destined for it, using a unique address known as the Media Access Control (MAC) address
	The card also performs error checking. Network cards are designed for specific types of networks and do not work on different network products.
	Different adapters may also support different connection speeds and connector types.

2.4 Internet service types.	
Fiber Optic	perform much better over long distances and are not affected by noise in the way that electrical signals over copper cable are.
Fiber to the Home (FTTH)	providing a fiber cable all the way to customer premises
	requires substantial investment by the telecom providers and is not widely available.
Fiber to the Curb (FTTC)	a compromise solution widely deployed in urban and some rural areas.
	provider has installed a fiber network terminating at a cabinet somewhere in a nearby street
	Each residence is connected to the fiber network over the ordinary copper telephone cabling using Very High Bit Rate DSL (VDSL)
Very High Bit Rate DSL (VDSL)	VDSL supports a downlink of up to 52 Mbps and an uplink of 16 Mbps at a distance of up to about 300m.
	VDSL2 also specifies a very short range (100m/300 feet) rate of 100 Mbps (bi-directional).
	The VDSL Internet modem/router is connected in much the same way as an ADSL modem/router.
Cable (Hybrid Fiber Coax)	usually provided as part of a Cable Access TV (CATV) service

2.4 Internet service types. (cont)	
	These networks are often described as Hybrid Fiber Coax (HFC) as they combine a fiber optic core network with coax links to customer premises equipment
	Coax is another type of copper cable but manufactured in a different way to twisted pair.
	The cable modem or modem/router is interfaced to the computer through an Ethernet adapter and to the cable network by a short segment of coax, terminated using an F-connector.
	Cable based on the Data Over Cable Service Interface Specification (DOCSIS) version 3.0 supports downlink speeds of up to about 1.2 Gbps.
Digital Subscriber Line (DSL)	one of the most popular SOHO Internet service types.
	works over an ordinary telephone line, providing the line is of sufficient quality
	modem/router is connected to the telephone line using a cable with RJ-11 connectors between the WAN port on the router and the telephone point
	Data is transferred over the line using the high frequency ranges that voice calls don't need to use.
ADSL (Asymmetric DSL)	the uplink (up to about 1.4 Mbps) is slower than the downlink (up to about 24 Mbps)
	The speeds achievable rely heavily on the quality of the telephone wiring and the distance to the local telephone exchange.
	The maximum supported distance is about three miles.

2.4 Internet service types. (cont)	
RF (Radio Frequency)	Radio waves propagate at different frequencies and wavelengths.
	Wi-Fi network products typically work at 2.4 GHz or 5 GHz
Satellite	System of microwave transmissions where orbital satellites relay signals between terrestrial receivers or other orbital satellites.
	Satellite internet connectivity is enabled through a reception antenna connected to the PC or network through a DVB-S modem.
Cellular Radio	data connections use radio transmissions but at greater range than Wi-Fi.
	more closely associated with Internet access for cell phones and smartphones than with computers.
	makes a connection using the nearest available transmitter (cell or base station).
	ach base station has an effective range of up to 5 miles (8 km)
	The transmitter connects the phone to the mobile and public switched telephone networks (PSTN)
	Cellular radio works in the 850 and 1900 MHz frequency bands (mostly in the Americas) and the 900 and 1800 MHz bands (rest of the world).
LTE (Long Term Evolution)	LTE is the cellular providers (3GPP) upgrade to 3G technologies such as W-CDMA and HSPA
	LTE Advanced is designed to provide 4G standard network access.
	developed in two competing formats, established in different markets: GSM (Global System for Mobile Communication)-allows subscribers to use a SIM (Subscriber Identity Module) card

2.4 Internet service types. (cont)

TIA/EIA IS-95 (cdmaOne)-based handsets. managed by the provider not the SIM. CDMA adoption is largely restricted to the telecom providers Sprint and Verizon.

2.5 Storage types.

Volatile Memory	stores data and computer programs that the CPU may need in real-time, and it erases them once a user switches off the computer.
	Dynamic RAM
	RAM(Random Access Memory)
	Cache
Non-Volatile Memory	Static memory - remains in a computer even after a user switches it off.
	HDD
	SSD
Local Storage Types:	
RAM (Random Access Memory)	Random Access Memory is the principal storage space for computer data and program instructions.
	RAM is generally described as being volatile in the sense that once power has been removed or the computer has been rebooted, data is lost.
DRAM (Dynamic RAM)	Dynamic RAM is a type of volatile memory that stores data in the form of electronic charges within transistors
	Due to the effects of leakage and the subsequent loss of electrical charge, DRAM has to be refreshed at regular intervals.
	Memory refreshing can be performed when the data bits are accessed regularly, but this periodic access slows down the operation of this memory type.
	Standard DRAM is the lowest common denominator of the DRAM types.
	Modern PCs use a DRAM derivative to store data (currently DDR2/3 SDRAM).
DDR SDRAM (Double Data Rate SDRAM)	Standard for SDRAM where data is transferred twice per clock cycle (making the maximum data rate [64+64] x the bus speed in bps).
	DDR2/DDR3 SDRAM uses lower voltage chips and higher bus speeds

2.5 Storage types. (cont)	
Flash Memory	Flash RAM is similar to a ROM chip in that it retains information even when power is removed, but it adds flexibility in that it can be reprogrammed with new contents quickly.
	has found a popular role in USB thumb drives and memory cards.
	These tiny cards can provide removable, megabyte or gigabyte storage for devices such as digital cameras.
	Other evolving uses of flash memory are in Solid State Drives (SSD), designed to replicate the function of hard drives, and hybrid drives (standard hard drives with a multigigabyte flash memory cache).
Blu-ray (Optical)	Latest generation of optical drive technology, with disc capacity of 25 GB per layer
	Transfer rates are measured in multiples of 36 MBps.
CD-ROM (Compact Disc - Read Only Memory) (Optical)	optical storage technology
	The discs can normally hold 700 MB of data or 80 minutes of audio data
	useful for archiving material
	Unlike magnetic media, the data on the disc cannot be changed (assuming that the disc is closed to prevent further rewriting in the case of RW media)
	This makes them useful for preserving tamper-proof records
UDF (Universal Disk Format)	File system used for optical media, replacing CDFS (ISO 9660).
Removable Media	In order to share files and programs, computers can either be connected to each other (across a direct link or via a network) or must be able store and retrieve files from an interim storage medium
	The most common types of removable media are floppy disks and optical discs
	However the term "removable media" also covers tape drives, high capacity disks, and removable hard drives

2.5 Storage types. (cont)	
HDD (Hard Disk Drive)(Static)	High capacity units typically providing persistent mass storage for a PC (saving data when the computer is turned off)
	Data is stored using platters with a magnetic coating that are spun under disk heads that can read and write to locations on each platter (sectors)
	A HDD installed within a PC is referred to as the fixed disks. HDDs are often used with enclosures as portable storage or as Network Attached Storage (NAS)
SSD (solid-state drive)	non-volatile storage media stores persistent data on solid-state flash memory
	significantly faster
	With an SSD, the device's operating system will boot up more rapidly, programs will load quicker and files can be saved faster.
	has no moving parts to break or spin up or down. The two key components in an SSD are the flash controller and NAND flash memory chips.
	read and write data to an underlying set of interconnected flash memory chips. These chips use floating gate transistors (FGTs) to hold an electrical charge, which enables the SSD to store data even when it is not connected to a power source. Each FGT contains a single bit of data, designated either as a 1 for a charged cell or a 0 if the cell has no electrical charge.
NAS (Network Attached Storage)	a storage device with an embedded OS that supports typical network file access protocols (TCP/IP and SMB for instance).
	These may be subject to exploit attacks (though using an embedded OS is often thought of as more secure as it exposes a smaller attack "footprint").
	The unauthorized connection of such devices to the network is also a concern.
File Server	In file server based networks, a central machine(s) provides dedicated file and print services to workstations.
	Benefits of server-based networks include ease of administration through centralization.

2.5 Storage types. (cont)

Cloud Computing	Any environment where software (Software as a Service and Platform as a Service) or computer/network resources (Infrastructure as a Service and Network as a Service) are provided to an end user who has no knowledge of or responsibility for how the service is provided.
	provide elasticity of resources and pay-per-use charging models.
	Cloud access arrangements can be public, hosted private, or private (this type of cloud could be onsite or offsite relative to the other business units).
Cloud--based Storage	There are also business-oriented solutions, such as DropBox and Amazon
	These services are typically operated with a browser or smartphone/tablet app.
	In Windows 10, a cloud storage client (OneDrive) is built into the OS and can be accessed via File Explorer.

2.6 Computing devices and their purposes

Mobile Device	Portable phones and smart phones can be used to interface with workstations using technologies such as Bluetooth or USB.
	As such, they are increasingly the focus of viruses and other malware
	Portable devices storing valuable information are a considerable security risk when taken offsite.
Tablet	A type of ultra-portable laptop with a touchscreen
	usually based on form factors with either 7" or 10" screens
	A phablet is a smaller device (like a large smartphone).
Laptop/Not-ebook	portable computer offering similar functionality to a desktop computer
	comes with built-in LCD screens and input devices (keyboard and touchpad)
	can be powered from building power (via an AC Adapter) or by a battery

2.6 Computing devices and their purposes (cont)	
	Peripheral devices can be connected via USB, PCMCIA, or ExpressCard adapters.
Workst-ation	type of PC is housed in a case that can sit on or under a desk
	often referred to as desktop PCs or just as desktops
Server	provides shared resources on the network and allows clients to access this information.
	The advantage of a server-based system is that resources can be administered and secured centrally.
	must be kept secure by careful configuration (running only necessary services) and maintenance (OS and application updates, malware/intrusion detection, and so on).
	Where a network is connected to the Internet, servers storing private information or running local network services should be protected by firewalls so as not to be accessible from the Internet.
Gaming Consoles	contains many of the same components as a workstation.
	have powerful CPUs and graphics processors, plus Ethernet and Wi-Fi for wired and wireless home networking and Internet connectivity
	Web cameras and microphones are also available as peripherals
	The main difference to a workstation is that a console is designed to be operated by a gaming pad rather than a keyboard and mouse, though these are often also available as options. A gaming console would use an HD (High Definition) TV for a display.
Internet of Things (IoT)	a world in which many different types of things are embedded with processing and networking functionality

2.6 Computing devices and their purposes (cont)

	Processing and networking functionality can be provisioned by very small chips, so the "things" can range from motor vehicles and washing machines to clothing and birthday cards.	
	The global network of personal devices (such as phones, tablets, and fitness trackers), home appliances, home control systems, vehicles, and other items that have been equipped with sensors, software, and network connectivity.	
Home Automation	from a clock to an alarm system or a refrigerator can be controlled over the Internet by home automation software	
	sitting at the heart of this automation, is a smart hub to which other devices connect	
	usually controlled using voice recognition systems and smartphone apps.	
	specific home automation product categories include:	Thermostats—monitor and adjust your home or office Heating, Ventilation, and Air Conditioning (HVAC) controls from an app installed on your phone.
		Security systems—monitor and control alarms, locks, lighting, and videophone entry systems remotely.
		IP cameras—often used for security, these devices connect to Internet Protocol (IP)-based networks such as the Internet and support direct upload and sync to cloud storage for remote monitoring.
		Home appliances—check the contents of your refrigerator from your smartphone while out shopping or start the washing machine cycle so that it has finished just as you get back to your house.

2.6 Computing devices and their purposes (cont)	
	Streaming media—play content stored on a storage device through any smart speaker or TV connected to the home network.
Medical devices	class of devices where use of electronics to remotely monitor and configure the appliance is expanding rapidly.
	hospitals and clinics but includes portable devices such as cardiac monitors/defibrillators and insulin pumps.
	allow doctors and nurses to remotely monitor a patient and potentially to adjust dosage levels or other settings without the patient having to visit the care provider.

2.7 Basic networking concepts	
IP (Internet Protocol)	Network (internet) layer protocol in the TCP/IP suite providing packet addressing and routing for all higher level protocols in the suite
Packet Transmiss-ion/Packet Switching Network	Packet switching introduces the ability for one computer to forward information to another.
	To ensure information reaches the correct destination, each packet is addressed with a source and destination address and then transferred using any available pathway to the destination computer
	A host capable of performing this forwarding function is called a router.
	described as "robust" because it can automatically recover from communication link failures.

2.7 Basic networking concepts (cont)

	It re-routes data packets if transmission lines are damaged or if a router fails to respond. It can utilize any available network path rather than a single, dedicated one.
	As well as the forwarding function and use of multiple paths, data is divided into small chunks or packets.
	Using numerous, small packets means that if some are lost or damaged during transmission, it is easier to resend just the small, lost packets than having to re-transmit the entire message.
DNS (Domain Name System)	This industry standard name resolution system provides name to IP address mapping services on the Internet and large intranets.
	DNS is a hierarchical, distributed database. DNS name servers host the database for domains for which they are authoritative.
	Root servers hold details of the top-level domains. DNS servers also perform queries or lookups to service client requests
	The DNS protocol defines the mechanisms by which DNS servers and clients interact
	The DNS protocol utilizes TCP/UDP port 53.
URL (Uniform Resource Locator/Identifier)	Application-level addressing scheme for TCP/IP, allowing for human-readable resource addressing

2.7 Basic networking concepts (cont)

	For example: protocol://server/file, where "protocol" is the type of resource (HTTP, FTP), "server" is the name of the computer (www.microsoft.com), and "file" is the name of the resource you wish to access.	
	The term URI (Uniform Resource Indicator) is preferred in standards documentation but most people refer to these addresses as URLs.	
A URL consists of the following parts:	Protocol	this describes the access method or service type being used. URLs can be used for protocols other than HTTP/HTTPS. The protocol is followed by the characters ://
	Host location	this could be an IP address, but as IP addresses are very hard for people to remember, it is usually represented by a Fully Qualified Domain Name (FQDN).
		DNS allows the web browser to locate the IP address of a web server based on its FQDN.
	File path	specifies the directory and file name location of the resource, if required
		Each directory is delimited by a forward slash.
		The file path may or may not be case-sensitive, depending on how the server is configured.
		If no file path is used, the server will return the default (home) page for the website.
WAN (Wide Area Network)	A Wide Area Network is a network that spans a relatively large geographical area, incorporating more than one site and often a mix of different media types and protocols.	

2.7 Basic networking concepts (cont)	
	Connections are made using methods such as telephone lines, fiber optic cables, or satellite links
LAN (Local Area Network)	A type of network covering various different sizes but generally considered to be restricted to a single geographic location and owned/managed by a single organization.
IP Address	Each IP host must have a unique IP address.
	This can be manually assigned or dynamically allocated (using a DHCP server).
	In IPv4, the 32-bit binary address is expressed in the standard four byte, dotted decimal notation: 10.0.5.1. In IPv6, addresses are 128-bit expressed as hexadecimal (for example, 2001:db8::0bcd:abcd:ef12:1234).
	IPv6 provides a much larger address space, stateless autoconfiguration (greatly simplifying network administration), and replaces inefficient broadcast transmissions with multicast ones.
MAC (Media Access Control) Address	A MAC is a unique hardware address that is hard-coded into a network card by the manufacturer
	This is required for directing data frames across a network and for allowing the network card to compare destination addresses (coded into the data frame) and its own unique MAC address.
	A MAC address is 48 bits long with the first half representing the manufacturer's Organizationally Unique Identifier (OUI)

2.7 Basic networking concepts (cont)	
HTTP	The protocol (HyperText Transfer Protocol) used to provide web content to browsers.
	HTTP uses port 80. HTTPS provides for encrypted transfers, using SSL and port 443
POP (Post Office Protocol)	TCP/IP application protocol providing a means for a client to access email messages stored in a mailbox on a remote server.
	The server usually deletes messages once the client has downloaded them. POP3 utilizes TCP port 110.
IMAP (Internet Message Access Protocol)	TCP/IP application protocol providing a means for a client to access email messages stored in a mailbox on a remote server.
	Unlike POP3, messages persist on the server after the client has downloaded them.
	IMAP also supports mailbox management functions, such as creating subfolders and access to the same mailbox by more than one client at the same time. IMAP4 utilizes TCP port number 143.
SMTP (Simple Mail Transfer Protocol)	The protocol used to send mail between hosts on the Internet. Messages are sent over TCP port 25
Modem (Modulator/D-emodulator)	Modems are devices that are used to convert the digital signals from a computer into the appropriate analog signal that is required for transmission over public phone lines - this is called modulation
	The reverse process, demodulation, occurs at the receiving computer

2.7 Basic networking concepts (cont)

	Modems are available in internal and external forms for different computer expansion slots and vary in terms of speed and data handling capabilities.
Router	Routers are able to link dissimilar networks and can support multiple alternate paths between locations based upon the parameters of speed, traffic loads, and cost.
	A router works at layer 3 (Network) of the OSI model. Routers form the basic connections of the Internet.
	They allow data to take multiple paths to reach a destination (reducing the likelihood of transmission failure)
	Routers can access source and destination addresses within packets and can keep track of multiple active paths within a given source and destination network.
	TCP/IP routers on a LAN can also be used to divide the network into logical subnets
Switch	Ethernet (or LAN) switches perform the functions of a specialized bridge.
	Switches receive incoming data into a buffer then the destination MAC address is compared with an address table.
	The data is then only sent out to the port with the corresponding MAC address.
	In a switched network, each port is in a separate collision domain and, therefore, collisions cannot occur. This is referred to as micros-egmentation.

2.7 Basic networking concepts (cont)

	Advanced switches perform routing at layers 3 (IP), 4 (TCP), or 7 (Application).
	Switches routing at layer 4/7 are referred to as load balancers and content switches.
AP (Access Point)	Device that provides connectivity between wireless devices and a cabled network.
	APs with Internet connectivity located in public buildings (cafes, libraries, airports for instance) are often referred to as hotspots.
Firewall	Hardware or software that filters traffic passing into or out of a network (for example, between a private network and the Internet)
	A basic packet-filtering firewall works at Layers 3 and 4 (Network and Transport) of the OSI model.
	Packets can be filtered depending on several criteria (inbound or outbound, IP address, and port number).
	More advanced firewalls (proxy and stateful inspection) can examine higher layer information, to provide enhanced security

2.8 Set up a wireless network

Wireless networking	generally understood to mean the IEEE's 802.11 standards for Wireless LANs (WLAN), also called Wi-Fi.
802.11n standard	an use either frequency band and deliver much improved data rates (nominally up to 600 Mbps)
802.11a and 802.11b,	supported data rates of 54 Mbps and 11 Mbps respectively.
802.11g	acted as an upgrade path for 802.11b, working at 54 Mbps but also allowing support for older 802.11b clients
802.11a	not as widely adopted but does use a less crowded frequency band (5 GHz) and is considered less susceptible to interf-erence than the 2.4 GHz band used by 802.11b/g.

2.8 Set up a wireless network (cont)

802.11ac	latest standardis now widely supported. 802.11ac access points can deliver up to 1.7 Gbps throughput at the time of writing. 802.11ac works only in the 5 GHz range with the 2.4 GHz band reserved for legacy standards support (802.11b/g/n).
Most SOHO routers support 802.11g/n or 802.11g/n/ac. This means that you can have a mix of client devices. For example, you might have a new router that supports 802.11ac but computers and tablets with wireless adapters that only support 802.11n. You can use the access point in compatibility mode to allow these devices to connect.	
Config-uring an Access Point	connect a PC or laptop to one of the LAN ports on the SOHO router.
	The SOHO router should assign the computer's adapter an Internet Protocol (IP) address using a service called the Dynamic Host Configuration Protocol (DHCP).
	Look at the SOHO router's setup guide to find out the router's IP address. Open a web browser and type the router's IP address into the address bar. This should open a management page for you to log on. Enter the user name and password listed in the router's setup guide. Most routers will invite you to complete the configuration using a wizard, which guides you through the process.
	Use the System page to choose a new admin password. The admin password is used to configure the router. It is vital that this password be kept secret and secure. You must choose a strong password that cannot be cracked by password-guessing software. Use a long, memorable phrase of at least 12 characters.
	(Use the System page to choose a new admin password. The admin password is used to configure the router. It is vital that this password be kept secret and secure. You must choose a strong password that cannot be cracked by password-guessing software. Use a long, memorable phrase of at least 12 characters.)
	Use the Wireless settings page to configure the router as an access point. Having checked the box to enable wireless communica-tions, you can adjust the following settings from the default.
	SSID (Service Set ID) - a name for the WLAN. This is usually set by default to the router vendor's name. It is a good idea to change the SSID from the default to something unique to your network. Remember that the SSID is easily visible to other wireless devices, so do not use one that identifies you personally or your address. The SSID can be up to 32 characters.

2.8 Set up a wireless network (cont)	
	Wireless mode—enable compatibility for different 802.11 devices.
Config-uring Wireless Security	To prevent snooping, you should enable encryption on the wireless network. Encryption scrambles the messages being sent over the WLAN so that anyone intercepting them is not able to capture any valuable information. An encryption system consists of a cipher, which is the process used to scramble the message, and a key. The key is a unique value that allows the recipient to decrypt a message that has been encrypted using the same cipher and key. Obviously, the key must be known only to valid recipients or the encryption system will offer no protection.
	under Encryption, you would select the highest security mode supported by devices on the network.
	WEP (Wired Equivalent Privacy)—this is an older standard. WEP is flawed and you would only select this if compatibility with legacy devices and software is imperative.
	Wi-Fi Protected Access (WPA)—this fixes most of the security problems with WEP. WPA uses the same weak RC4 (Rivest Cipher) cipher as WEP but adds a mechanism called the Temporal Key Integrity Protocol (TKIP) to make it stronger.
	WPA2—this implements the 802.11i WLAN security standard. The main difference to WPA is the use of the AES (Advanced Encryption Standard) cipher for encryption. AES is much stronger than RC4/TKIP. The only reason not to use WPA2 is if it is not supported by devices on the network. In many cases, devices that can support WPA can be made compatible with WPA2 with a firmware or driver upgrade.
attenu-ation	The distance between the wireless client (station) and access point determines the attenuation (or loss of strength) of the signal
interf-erence	Radio signals pass through solid objects, such as ordinary brick or drywall walls but can be weakened or blocked by particularly dense or thick material and metal. Other radio-based devices and nearby Wi-Fi networks can also cause interference
Captive Portal	A web page or website to which a client is redirected before being granted full network access

2.8 Set up a wireless network (cont)

The portal might allow limited network browsing, provide an authentication mechanism, or provide resources, such as access to patches or signature updates to allow the device to become compliant with network access policies. It can also function as a secondary authentication mechanism for open access points.

On connecting, the user's browser is redirected to a server to enter credentials (and possibly payment for access).

3.1 Purpose of operating systems.

Applic-ation	a program, or group of programs, that allow users to perform different tasks, such as web browsing, email, and word processing
	With an OS, application software developers do not need to worry about writing routines to access the hard disk or send a document to a printer; they simply "call" functions of the OS that allow them to do these things.
	This allows application software designers to concentrate on application functions and makes the computer more reliable
	One consequence of this is that there are relatively few operating systems, as it takes a lot of work to produce software applications that will work with different systems
	Application vendors have to decide which operating systems they will support.
Hardware	Each hardware component requires a driver to wor
	OS software is built from a kernel of core functions with additional driver software and system utility applications

3.1 Purpose of operating systems. (cont)

	The OS is responsible for identifying the components installed on the PC and loading drivers to enable the user to configure and use them.
SOHO (Small Office Home Office)	Typically used to refer to network devices designed for small-scale LANs (up to 10 users).
Kernel	All operating systems have a kernel
	which is a low-level piece of code responsible for controlling the rest of the operating system
	Windows uses a multiprocessor aware, pre-emptive multitasking kernel.
Mobile device OS	designed for handheld devices, such as smartphones and tablets.
Android	Mobile (smartphone and tablet) OS developed by the Open Handset Alliance (primarily sponsored by Google). Android is open source software.
iOS	Mobile OS developed by Apple for its iPhone and iPad devices
OS X	Operating system designed by Apple for their range of iMac computers, Mac workstations, and MacBook portables
	OS X is based on the BSD version of UNIX
	OS X is well supported by application vendors, especially in the design industry (Adobe/Macromedia).
Chrome OS	derived from Linux, via an open source OS called Chromium
	Chrome OS itself is proprietary

3.1 Purpose of operating systems. (cont)		
	developed by Google to run on specific laptop (chromebooks) and PC (chromeboxes) hardware.	
Linux	An open-source operating system supported by a wide range of hardware and software vendors	
Microsoft	world's foremost supplier of operating system and Office productivity software	
	dominated the PC market since the development of the first IBM compatible PCs running MS-DOS.	
Workstation OS	runs a traditional desktop PC or laptop. Examples include Microsoft Windows, Apple OS X/macOS, Linux, and Chrome OS.	
	The general workstation OS types are:	Enterprise client—designed to work as a client in business networks
		Home client—designed to work on standalone or workgroup PCs and laptops in a home or small office. This will also allow each client to run some basic peer-to-peer network services, such as file sharing.
Network Operating System (NOS), or server OS	designed to run on servers in business networks	
	A server OS, such as Windows Server, Linux, or UNIX, is often based on similar code to its workstation OS equivalent.	
	For example, Windows 10 and Windows Server 2016 are very similar in terms of the OS kernel.	
	A server OS is likely to include software packages (or roles) to run network services and use different licensing to support more users.	

3.1 Purpose of operating systems. (cont)

	A server OS is also likely to have a simpler command-line interface, rather than a GUI, to make it more secure and reliable.
Embedded OS	a computer or appliance designed for a very specific function.
	hese systems can be as contained as a microcontroller in an intravenous drip-rate meter or as large and complex as an industrial control system managing a water treatment plant.
	Embedded systems are typically static environments. A PC is a dynamic environment
Firmware	refers to software instructions stored semi-permanently (embedded) on a hardware device (BIOS instructions stored in a ROM chip on the motherboard for instance).
Hypervisor	also known as a virtual machine monitor or VMM
	software that creates and runs virtual machines (VMs)
	allows one host computer to support multiple guest VMs by virtually sharing its resources, such as memory and processing.
Hypervisor Type 1	“bare metal”
	acts like a lightweight operating system and runs directly on the host's hardware
Hypervisor Type 2	runs as a software layer on an operating system, like other computer programs
Disk Management	Disk management • Process management/scheduling (Kill process/end task) • Memory management • Access control/protection

3.1 Purpose of operating systems. (cont)

	The Disk Management snap-in displays a summary of any fixed and removable drives attached to the system. The top pane lists drives; the bottom pane lists disks, showing information about the partitions created on each disk plus any unpartitioned space. You can use the tool to create and modify partitions, reformat a partition, assign a different drive letter, and so on.
	one of the snap-ins included with the default Computer Management console
	you can open the tool directly from the Windows+X menu (or run diskmgmt.msc).
Partitions	allows a single disk to be divided into multiple different logical areas, each of which can be accessed via the OS as a separate drive.
	A disk must have at least one partition for the OS to use it.
	each partition must be formatted with a file system so that the OS can read and write files to the drive.
Process	When a program starts (either because it has been scheduled to do so by the OS or opened by a user), the application code executes in memory as a process
Task Manage-r(t-askmgr)	allows the user to shut down processes that are not responding.
	An ordinary user can end unresponsive applications, but administrative rights are required to end processes that were started by the system rather than the signed in user

3.1 Purpose of operating systems. (cont)	
	This protects the system as things like malware cannot disable anti-virus software
	In addition to this functionality, Task Manager can be used to monitor the PC's key resources.
	There are various ways to run Task Manager, including pressing CTRL+SHIFT+ESC, right-clicking the taskbar, right-clicking the Start button, or pressing Windows+X.
taskkill	Terminating a process like this (rather than using the application's Close or Exit function) is often called "killing" the process.
	The command line option for doing this in Windows is indeed called taskkill
	Always try to close or end a task normally before attempting to "kill" it.
Service	a Windows process that does not require any sort of user interaction and thus runs in the background (without a window).
	provide functionality for many parts of the Windows OS, such as allowing sign in, browsing the network, or indexing file details to optimize searches
	may be installed by Windows and by other applications, such as anti-virus, database, or backup software.
	use this snap-in to check which services are running and to start and stop each service or configure its properties, such as whether it starts automatically at system boot time.

3.1 Purpose of operating systems. (cont)	
Task Scheduler	sets tasks to run at a particular time.
	Tasks can be run once at a future date or time or according to a recurring schedule
	A task can be a simple application process (including a command with any options if necessary) or a batch file, also called a script (a file that contains commands).
	accessed via its own console and can also be found in the Computer Management console.
	In Linux, the cron utility is often used to run tasks or scripts at a particular time.
Memory Management	When a process executes, it takes up space in system memory.
	If the system runs out of memory, then processes will be unable to start, and running processes may crash because they cannot load the data they need.
	There is not a lot to configure in terms of memory management.
	Badly written programs and malware can cause a memory leak, where the process keeps claiming memory addresses without releasing them
	If the system keeps running out of memory, you would use Task Manager or another monitoring program to find the offending process and disable it from running.
Access control	means that a computing device (or any information stored on the device) can only be used by an authorized person, such as its owner.

3.1 Purpose of operating systems. (cont)	
	on workstation operating systems is usually enforced by the concept of user accounts
	Each user of the device is allocated an account and uses a password (or other credential) to authenticate to that account.
	The OS can restrict the privileges allocated to an account so that it is not able to reconfigure settings or access certain data areas.
Administrator account	When the OS is first installed, the account created or used during setup is a powerful local administrator account
	you should only use this account to manage the computer (install applications and devices, perform troubleshooting, and so on).
Standard users group	You should create ordinary user accounts for day-to-day access to the computer
	cannot change the system configuration and are restricted to saving data files within their own user profile folder or the Public profile.
Least privilege principle	users should have only sufficient permissions required to perform tasks and no more.
User Account Control (UAC)	Windows' solution to the problem of elevated privileges
	In order to change important settings on the computer (such as installing drivers or software), administrative privileges are required.
Device management	Primary interface for configuring and managing hardware devices in Windows.

3.1 Purpose of operating systems. (cont)

Device Manager enables the administrator to disable and remove devices, view hardware properties and system resources, and update device drivers.

You can open Device Manager via the Windows+X menu, locate the device, then right-click and select Uninstall

Or via the Computer Management Console

3.2 Components of an operating system

Services	See 3.1
Processes	See 3.1
Task Scheduler	The Task Scheduler enables the user to perform an action (such as running a program or a script) automatically at a pre-set time or in response to some sort of trigger.
Computer Management Console	The Computer Management Console provides tools for administering the local computer, including Device Manager, Event Viewer, Disk Management, Services, and Performance Monitor
Command Line Interfaces	The Computer Management Console provides tools for administering the local computer, including Device Manager, Event Viewer, Disk Management, Services, and Performance Monitor.
	represents an alternative means of configuring an OS or application to a GUI
	To access the console, alt-click (My) Computer and select Manage.
	displays a prompt, showing that it is ready to accept a command.

3.2 Components of an operating system (cont)	
	When you type the command plus any switches and press ENTER, the shell executes the command, displays any output associated with the execution, and then returns to the prompt.
GUI (Graphical User Interface)	A GUI provides an easy to use, intuitive interface for a computer operating system
	m. Most GUIs require a pointing device, such as a mouse, to operate efficientl
Device Driver	A small piece of code that is loaded during the boot sequence of an operating system.
	This code, usually provided by the hardware vendor, provides access to a device, or hardware, from the OS kernel.
	. Under Windows, a signing system is in place for drivers to ensure that they do not make the OS unstable.
Plug-and-Play (PnP)	A Plug-and-Play system (comprising a compatible BIOS, operating system, and hardware) is self-configuring
	When a hardware device is added or removed, the operating system detects the change and automatically installs the appropriate drivers.
Driver update	Device Manager provides the interface for configuring and managing hardware devices in Windows.
	In the Device Manager, the admin can disable and remove devices, view hardware properties and systems resources, and update device drivers

3.2 Components of an operating system (cont)	
	Windows ships with a number of default drivers and can also try to locate a driver in the Windows Update website
	third-party drivers should be obtained from the vendor's website
	To update, you download the driver files and install them using the supplied setup program or extract them manually and save them to the hard disk. You can then use the device's property dialog in Device Manager to update the driver. You can either scan for the update automatically or point the tool to the updated version you saved to the hard disk.
TWAIN	Standard "driver" model for interfacing scanner hardware with applications software.
WIA (Windows Image Acquis-ition)	Driver model and API (Application Programming Interface) for interfacing scanner hardware with applications software on Windows PCs
File System	When data is stored on a disk, it is located on that medium in a particular, standardized format.
	This allows the drive and the computer to be able to extract the information from the disk using similar functions and thus data can be accessed in a predictable manner
	r. Examples of file systems include FAT16, FAT32, and NTFS (all used for hard disks) and CDFS (ISO 9660) and UDF (Universal Disk Format), used for optical media such as CD, DVD, and Blu-ray.

3.2 Components of an operating system (cont)	
Partition	A discrete area of storage defined on a hard disk using either the Master Boot Record (MBR) scheme or the GUID Partition Table (GPT) scheme.
	Each partition can be formatted with a different file system, and a partition can be marked as active (made bootable).
NTFS (New Technology Filing System)	The NT File System supports a 64-bit address space and is able to provide extra features such as file-by-file compression and RAID support as well as advanced file attribute management tools, encryption, and disk quotas
FAT (File Allocation Table)	When a disk is formatted using the FAT or FAT32 file system a File Allocation Table (FAT) is written in a particular track or sector
	r. The FAT contains information relating to the position of file data chunks on the disk; data is not always written to one area of the disk but may be spread over several tracks.
	The original 16-bit version (FAT16, but often simply called FAT) was replaced by a 32-bit version that is almost universally supported by different operating systems and devices.
	A 64-bit version (exFAT) was introduced with Windows 7 and is also supported by XP SP3 and Vista SP1 and some versions of Linux and OS X.
Hierarchical File System (HFS+)	Apple Mac workstations and laptops use the extended Hierarchical File System (HFS+)
	the latest macOS version is being updated to the Apple File System (APFS)

3.2 Components of an operating system (cont)	
ext	Most Linux distributions use some version of the ext file system to format partitions on mass storage devices.
	ext3 is a 64-bit file system with support for journaling, which means that the file system tracks changes, giving better reliability and less chance of file corruption in the event of crashes or power outages
	Support for journaling is the main difference between ext3 and its predecessor (ext2).
	ext4 delivers significantly better performance than ext3 and would usually represent the best choice for new systems.
exFAT	can be used where the NTFS file system is not a feasible solution (due to data structure overhead), but require a greater file size limit than the standard FAT32 file system (i.e. 4 GiB).
	exFAT has been adopted by the SD Card Association as the default file system for SDXC cards larger than 32 GiB
	Along with most of the features of NTFS, less overhead means faster processing for the exFAT file system, making it particularly suitable for flash drives.
Compression Software	To send or store a file it often needs to be compressed in some way, to reduce the amount of space it takes up on the storage media or the bandwidth required to send it over a network
	There are a number of compression utilities and formats

3.2 Components of an operating system (cont)		
Compression Formats	zip	this format was developed for the PKZIP utility but is now supported "natively" by Windows, Mac OS X, and Linux.
		"Natively" means that the OS can create and extract files from the archive without having to install a third-party application
	tar	this was originally a UNIX format for writing to magnetic tape (tape archive) but is still used with gzip compression (tgz or .tar.gz) as a compressed file format for UNIX, Linux, and macOS.
		A third-party utility is required to create and decompress tar files in Windows.
	rar	this proprietary format is used by the WinRAR compression program.
	7z	this type of archive is created and opened using the open-source 7-Zip compression utility
	gz	this type of archive is created and opened by the gzip utility, freely available for UNIX and Linux computers.
		A number of Windows third-party utilities can work with gzip-compressed files.
	iso	this is a file in one of the formats used by optical media. The main formats are ISO 9660 (used by CDs) and UDF (used by DVDs and Blu-Ray Discs)
		Many operating systems can mount an image file so that the contents can be read through the file browser.
	vhd/vmdk	these are disk image file formats used with Microsoft Hyper-V and VMware virtual machines respectively.

3.2 Components of an operating system (cont)

	A disk image is a file containing the contents of a hard disk, including separate partitions and file systems
	Like an ISO, such a file can often be mounted within an OS so that the contents can be inspected via the file browser.
dmg	this is a disk image file format used by Apple macOS.
Encryption	Scrambling the characters used in a message so that the message can be seen but not understood or modified unless it can be deciphered
	Encryption provides for a secure means of transmitting data and authenticating users.
	It is also used to store data securely
	Encryption systems allow for different levels of security (128-bit encryption is currently considered secure).
Key (Encry-ption)	An encryption cipher scrambles a message (plaintext) using an algorithm
	The algorithm is given a key so that someone intercepting the message could not just reverse the algorithm to unscramble the message; they must also know the key. In symmetric encryption, the same key is used for encryption and decryption
	In asymmetric encryption, different keys are used (one key is linked to but not derivable from the other key).
Full device encryption	Provided by all but the early versions of mobile device OS for smartphones and tablets, such as Android and iOS

3.2 Components of an operating system (cont)	
iOS 5 (and up) Levels of Encryption	All user data on the device is always encrypted, but the key is stored on the device. This is primarily used as a means of wiping the device. The OS just needs to delete the key to make the data inaccessible rather than wiping each storage location.
	Email data and any apps using the "Data Protection" option are also encrypted using a key derived from the user's passcode (if this is configured). This provides security for data in the event that the device is stolen. Not all user data is encrypted; contacts, SMS messages, and pictures are not, for example.
Data Protection encryption	iOS
	enabled automatically when you configure a password lock on the device
	In Android, you need to enable encryption via Settings > Security. Android uses full-disk encryption with a passcode-derived key. When encryption is enabled, it can take some time to encrypt the device.
Permissions	To access files and folders on a volume, the administrator of the computer will need to grant file permissions to the user (or a group to which the user belongs)
	File permissions are Page 9/16 supported by NTFS-based Windows systems
AAA	Authentication, Authorization, and Accounting - the principal stages of security control. A resource should be protected by all three types of controls.

3.2 Components of an operating system (cont)	
ACL (Access Control List)	The permissions attached to or configured on a network resource, such as folder, file, or firewall
	The ACL specifies which subjects (user accounts, host IP addresses, and so on) are allowed or denied access and the privileges given over the object (read only, read/write, and so on).
Group Account	A group account is a collection of user accounts
	These are useful when establishing file permissions and user rights because when many individuals need the same level of access, a Page 15/16 group could be established containing all the relevant users
	The group could then be assigned the necessary rights.
MAC (Mandatory Access Control)	Access control model where resources are protected by inflexible, system defined rules
	Resources (objects) and users (subjects) are allocated a clearance level (or label)
	Resources (objects) and users (subjects) are allocated a clearance level (or label)
File naming rules	Naming rules depend on the version of Windows and the file system
	A file name can be up to 255 characters long and can contain letters, numbers, and underscores.
	The operating system is case-sensitive, which means it distinguishes between uppercase and lowercase letters in file names. Therefore, FILEA, FiLea, and filea are three distinct file names, even if they reside in the same directory.

3.2 Components of an operating system (cont)

	File names should be as descriptive and meaningful as possible.
	Directories follow the same naming conventions as files.
	Certain characters have special meaning to the operating system. Avoid using these characters when you are naming files. These characters include the following: / \ " ' * ; - ? [ ] ( ) ~ ! $ { } < > # @ & | space tab newline
	A file name is hidden from a normal directory listing if it begins with a dot (.). When the ls command is entered with the -a flag, the hidden files are listed along with regular files and directories.
Directory	A file system object used to organize files
	Directories can be created on any drive (the directory for the drive itself is called the root) and within other directories (subdirectory)
	Different file systems put limits on the number of files or directories that can be created on the root or the number of subdirectory levels.
	In Windows, directories are usually referred to as folders.
File	Data used by a computer is stored by saving it as a file on a disk
	Files store either plain text data or binary data
	Binary data must only be modified in a suitable application or the file will be corrupted
	A file is created by specifying a name
	Files usually have a three character extension (the last 3 characters in the file named preceded by a period)

3.2 Components of an operating system (cont)	
	The file extension is used to associate the file with a particular software application
	Files have primary attributes (Read-Only, System, Hidden, and Archive) and other properties (date created or modified for instance)
	Files stored on an NTFS partition can have extended attributes (access control, compression, and encryption).
8.3 Filenames	The DOS file naming standard - an eight-character ASCII name followed by a three-character file extension (which identifies the file type).
	Windows supports long file names but can also generate a short file name, based on DOS 8.3 naming rules.
	. This provides backwards compatibility for older applications.
File Permissions	supported by NTFS-based Windows systems.

3.3 Purpose and proper use of software		
Productivity software	Word processing	applications that help users to write and edit documents
		will come with features enabling the user to edit, format, and review text quickly.
	Spreadsheet	A spreadsheet consists of a table containing rows, columns, and cells
		When values are entered into the cells, formulas can be applied to them, enabling complex calculations to be carried out.
	Presentation	Presentation software enables users to create sophisticated business presentations that can be displayed as an on-screen slide show or printed onto overhead projector transparencies.

3.3 Purpose and proper use of software (cont)		
	Browser	A web browser is software designed to view HTML pages.
		Browsers must be configured carefully and kept up to date with system patches to make them less vulnerable to Trojans and malicious scripting.
		As well as the browser itself, plug-in applications that enable use of particular file formats, such as Flash or PDF, may also be vulnerable.
	Visual diagramming	Diagrams are an important means of communicating or recording ideas or configurations clearly
		software assists the creation of these by providing templates and shapes for different kinds of diagram.
		user does not have to worry about creating icons or shapes; they can just drag shapes from the template (or stencil) into the diagram and use the software tools to connect them appropriately.
Collab-oration software	Email client	The email client software works in conjunction with an email server, which handles the business of actually transmitting the messages over the network.
		often coupled with a Personal Information Manager (PIM). PIM software provides features for storing and organizing information, such as contacts and calendar events and appointments.
	Online Workspaces and Document Storage/S-haring	where a file is hosted on a network, and users can sign in to get access to it.
		Different users might be assigned different permissions over the document. For example, some users may be able to view or print the document or add comments to it; others may be able to edit it.

3.3 Purpose and proper use of software (cont)

	The client software provides the user with the tools to view and edit the document.
Remote Desktop and Screen Sharing Software	allows a user to connect to a computer over a network.
	The remote desktop server runs on the target computer.
	The user starts a remote desktop client application and enters the connection information.
	When the connection is established, the user can operate the remote computer's desktop via a window on their local computer
	also used by IT support staff to login to a user's computer to provide support and assistance without having to travel to the user's location.
	Remote connection utilities can also be used in a "read-only" type of mode to facilitate screen sharing. the remote user can view the host's desktop but cannot interact with it. This mode is often used for software demonstrations and for product support.
Instant Messaging	Instant Messaging (IM) software allows users to communicate in real time. Unlike with email, there is (virtually) no delay between sending and receiving a message. Basic IM software allows for the transfer of text messages and can also be used for file attachments.
VoIP Software	packages voice communications as data packets, transmits them over the network, then reassembles the packets to provide two-way, real-time voice communication.
	"Real-time" applications such as IM are sensitive to latency, which is the delay in seconds that a packet of data takes to travel over a network

3.3 Purpose and proper use of software (cont)		
		IM voice and video calling also requires sufficient bandwidth
		These factors might be controllable on a private network, but on the Internet, where a packet might traverse many different networks to reach its final destination, link quality is more difficult to guarantee.
	Video Conferencing	Video conferencing or Video Teleconferencing (VTC) software allows users to configure virtual meeting rooms, with options for voice, video, and instant messaging. Other features often include screen sharing, presentation/whiteboard, file sharing, and polls and voting options.
		Most conferencing suites also provide a fallback teleconference option, to be used in conjunction with the presentation features, in case some participants cannot get a good enough connection for an IP voice or video call.
	Telepresence	a term used to refer to particularly sophisticated video conferencing solutions
		participants have a real sense of being in the same room
		can be achieved by a number of video technologies, including HD or 4K resolutions, large and/or curved flat-screens, and 3D. Emerging technologies might make use of virtual reality headsets, holograms, and robotics.
Business Software	Desktop Publishing (DTP	similar to word processing but with more emphasis on the formatting and layout of documents than on editing the text. DTP software also contains better tools for preparing a document to be printed professionally.
	Graphic Design	Often used in conjunction with DTP and web design software

3.3 Purpose and proper use of software (cont)	
Computer Aided Design (CAD)	makes technical drawings and schematics easier to produce and revise.
	Drawings can be rotated or viewed in 3D and easily transmitted to a client for feedback
	often linked to Computer Aided Manufacturing (CAM) which enables the data produced in CAD drawings to be loaded into a machine which then manufactures the part.
Project Management	involves breaking a project into a number of tasks and assigning responsibilities, resources, and timescales to ensure the completion of those tasks
	also involves identifying dependencies between tasks.
	Software such as Microsoft Project or Smartsheet assists with this process by visualizing task timelines and dependencies and recording information about task properties and progress.
Database	enable the user to store, organize, and retrieve information.
	can search through thousands of records very quickly and display data in a format specified by the user
	can be used to store many different types of information, such as timetables, customer details, and patient records.
	The XML (eXtensible Markup Language) format is also increasingly important for data storage, as it allows for a high level of integration between different types of systems.
Business-specific	A company may also commission custom-made software to implement specific Line of Business (LOB) functions
	LOB applications would cover functions that cannot be performed by "off-the-shelf" software.

3.3 Purpose and proper use of software (cont)

This might include product design and manufacturing, fulfilment and inventory control, plus marketing and sales.

3.4 App architecture & delivery models

Application Delivery Methods	Locally installed	Network not required, Application exists locally, Files saved locally
		A traditional PC-type software application is installed locally to the computer's hard drive.
		When launched it executes within the computer's memory and is processed by the local CPU.
		Any data files manipulated by the application can also be stored on the local disk, though usually in a user folder rather than the application folder.
		or security reasons ordinary users should not be able to modify application folders.
		A locally installed application such as this does not need network access to run, though obviously the network has to be present if the application makes use of network features.
	Local network hosted	Network required, Internet access not required
		application installed to a network server and executed on that server.
		client workstations access the application using a remote terminal or viewer.
		The most successful example of this kind of application virtualization model is Citrix XenApp. Locating the application and its data files on a server is easier to secure and easier to backup.
		This model also does not require that client hosts be able to access the Internet
		The drawback is that if there is no local network connection or the local network is heavily congested, users will not be able to use the application.

3.4 App architecture & delivery models (cont)		
	Cloud hosted	Internet access required, Service required, Files saved in the cloud
		very similar to the local network model except that clients connect to the application servers over the Internet.
		provides a lot of flexibility in terms of provisioning the app to clients located in different regions
		As with local network applications, user-generated data files would normally be saved in the cloud too, with the same benefits for creating security access controls and backing up easily.
		The drawback is that clients and cloud service must both have a reliable Internet connection. Outages on either side can cause serious productivity problems.
Application architecture models	One tier(s-tandalone)	front-end and processing logic and the database engine are all hosted on the same computer
	Two-tier	separates the database engine, or back-end or data layer, from the presentation layer and the application layer, or business logic
		The application and presentation layers are part of the client application.
		The database engine will run on one server (or more likely a cluster of servers), while the presentation and application layers run on the client.
	Three-tier	the presentation and application layers are also split
		The presentation layer provides the client front-end and user interface and runs on the client machine
		The application layer runs on a server or server cluster that the client connects to.

3.4 App architecture & delivery models (cont)

	When the client makes a request, it is checked by the application layer, and if it conforms to whatever access rules have been set up, the application layer executes the query on the data layer which resides on a third tier and returns the result to the client.
	The client should have no direct communications with the data tier.
n-tier	used to mean either a two-tier or three-tier application, but another use is an application with a more complex architecture still
	For example, the application may use separate access control or monitoring services.

3.5 Configure & use web browsers

Caching/c-learing cache	privacy issue is that the browser can be set to store information typed into forms, including passwords, and retains a history of browsed pages
	Any user using a publicly accessible computer should be trained to check these settings and to clear the browser cache before logging off.
	This is done from the browser's settings dialog or configuration page.
Private Browsing Mode	the browser doesn't store cookies or temporary files and doesn't add pages to the history list
	does allow the creation of cookies but only ones that are directly connected to the URL you are visiting. It also deletes the cookies when you close the page. Third-party cookies are not accepted.

3.5 Configure & use web browsers (cont)

	Private mode does not stop the browser from sending some information to the website. You cannot avoid the website discovering your IP address for instance. For fully "anonymous" browsing, you have to use some sort of Virtual Private Network (VPN) or proxy.
	You can usually open a private browser tab by pressing CTRL+SHIFT+P (in Firefox) or CTRL+SHIFT+N (in Chrome).
Deactivate Client-side Scripting	Most sites will use server-side scripting, meaning that code runs on the server to display the page you are looking at.
	Many sites also depend on client-side scripting, so there is no way to disable this.
	This means that code is placed in the page itself and runs within the browser to change the way it looks or provide some other functionality.
	Deactivating client-side scripting tends to break most of the websites published on the Internet because they depend very heavily on the functionality that scripting allows.
	Scripting can be disabled in some browsers by configuring settings, but others, Microsoft's new Edge browser for instance, do not allow scripts to be disabled.
	It is also possible to install a script blocker add-on. This provides more control over which websites are allowed to run scripts.

3.5 Configure & use web browsers (cont)

Browser add-ons/e-xtensions	Add-ons come in several different types:	Extensions—these can add functionality to the browser. They might install a toolbar or change menu options. They can run scripts to interact with the pages you are looking at.
		Plug-ins—these are designed to play some sort of content embedded in a web page, such as Flash, Silverlight, or other video/multimedia format. The plug-in can only interact with the multimedia object placed on the page, so it's more limited than an extension
		Themes—these change the appearance of the browser using custom images and color schemes.
	You can view installed add-ons and choose to remove or enable/disable them using the browser settings button or menu.	
	All extensions and plug-ins should be digitally signed by the developer to indicate that the code is as-published. You should be extremely wary of installing unsigned add-ons.	
	about:addons allows you to add, remove, enable/disable addons	
Proxy settings	a network firewall is likely to be deployed to monitor and control all traffic passing between the local network and the Internet. On networks like this, clients might not be allowed to connect to the Internet directly but forced to use a proxy server instead	
	The proxy server can be configured as a firewall and apply other types of content filtering rules.	

3.5 Configure & use web browsers (cont)		
	Some proxy servers work transparently so that clients use them without any extra configuration of the client application	
	Other proxies require that client software, such as the browser, be configured with the IP address and port of the proxy server.	
	This information would be provided by the network administrator.	
Certificates (Valid, Invalid)	When you browse a site using a certificate, the browser displays the information about the certificate in the address bar:	
	If the certificate is valid and trusted	a padlock icon is shown
		Click the icon to view information about the certificate and the Certificate Authority guaranteeing it.
	f the certificate is highly trusted	the address bar is colored green
		High assurance certificates make the website owner go through a (even) more rigorous identity validation procedure
	If the certificate is untrusted or otherwise invalid	the address bar is colored maroon and the site is blocked by a warning message
		If you want to trust the site anyway, click through the warning.
pop-up	a "sub-window" that appears over the main window	
	can be implemented using scripts or add-ons	
	can be opened automatically by a script running on the page or in response to clicking a link	
	Aggressive use of pop-up windows is associated with spyware and adware	

3.5 Configure & use web browsers (cont)

	These spawn pop-ups when you open the browser, on every site you visit, and when you try to close the browser. They may even re-spawn when you try to close them
Popup blockers	You can control the use of cookies by the websites you visit using browser settings.
	You can also choose to prevent sites from creating pop-up windows and configure exceptions for this rule. Note that this will not block all types of overlay pop-ups or advertising.
	If you want to have closer control over advertising on a site you need to install a suitable browser extension.
Compatible Browser	It is often the case that you will need to have more than one browser installed on your computer.
	This is not ideal in security terms, as it is better to install as few applications as possible, but circumstances may demand it.
	Compatibility aside, your choice of browser is largely down to personal preference.
	Do make sure you choose a browser whose developer is active in monitoring security issues and providing software updates to fix them.

3.6 General application concepts & uses

Licensing	Terms governing the installation and use of operating system and application software	A license may cover use on a single computer or by a number of devices or concurrent users at a site.
	When you buy software, you must read and accept the license governing its use, often called the End User License Agreement (EULA).	

3.6 General application concepts & uses (cont)	
	terms of the license will vary according to the type of software
Single use	the basic restriction is usually that the software may only be installed on one computer
Group use/site license	the company can install the software on an agreed number of computers for an unlimited number of employees to use at the same time
Concurrent license	the company can allow only a set number of users access to it at any one time.
	It is important to monitor usage of the software to ensure that the permitted number of host-installs or concurrent users is not exceeded.
Client Access Licenses (CAL)	software bought under license can be installed onto a network server so that all authorized users can access it without it being installed on each individual computer
One-time purchases	give perpetual use of the software, though subsequent upgrades would normally involve a new license fee
	This model is being replaced by subscription-based licensing
Subscription-based licensing	organizations pay a per-user monthly fee to get access to the software.
	upgrades are provided as part of the subscription
Open Source	Open source means that the programming code used to design the software is freely available.
	other programmers can investigate the program and make it more stable and usefu

3.6 General application concepts & uses (cont)		
	An open source license does not forbid commercial use of applications derived from the original, but it is likely to impose the same conditions on further redistributions.	
Shareware	software that you can install free of charge so that you can evaluate it for a limited period	
	If you decide to continue using the software after this period, you must register it, usually for a fee.	
	When you register the software, you often become entitled to extra features and support.	
Freeware	software that is available free of charge	
product key	A product key is often used to authenticate the use of a software package and may be required to activate the software for use.	
	a long string of characters and numbers printed on the box or disk case	
	The product key will generate a different product ID or serial number, which is often used to obtain technical support	
Reading Instructions and Documentation	Before you try to install an application, make sure you are following software installation best practices	
	Read the accompanying documentation to verify:	That the software is compatible with your operating system.
		That your computer hardware meets the application's recommended system requirements.
		Any special installation instructions or known issues.

3.6 General application concepts & uses (cont)	
	That you have a valid agreement or license to install and use the product.
Advanced Options Advanced Options	Most software installer packages offer a choice between a default installation and a custom (or advanced options) installation.
	A custom installation allows you to choose specific settings, such as where to install the software and what icons or startup/autorun options to configure
	A custom installation may also involve the selection of specific feature sets or modules within the software package.
Software Agreement	how any data gathered and processed by the software is used, stored, and retained by the software vendor.
Single-platform Software	this model produces software that is optimized for a particular platform, it can perform better and be simpler to check for errors than cross-platform software.
	The drawback is that "porting" the software to a different platform (from Windows OS to Android for instance) can be very difficult
Cross-platform Software	any software application that works on multiple operating systems or devices, often referred to as platforms
	you can use the same program, whether on a Windows PC or logging in from your laptop or smartphone

3.6 General application concepts & uses (cont)

you'll be more productive and be able to use a software product you're familiar with regardless of the operating system or device you choose

your files can be moved much more easily between your devices and can use the software with whatever device you have with you

Using a cloud connection, there's a way to keep all of your work in sync across your devices.

Compatibility issues can also affect web applications as different browser vendors can make slightly different interpretations of open standards that result in applications not working correctly in particular browsers or browser versions.

4.1 Programming language categories

Assembly Language	A compiled software program is converted to binary machine code using the instruction set of the CPU platform.
	typically specific to a particular hardware architecture.
	Assembly language is this machine code represented in humanreadable text
	This is in contrast to compiled, interpreted, and query languages which you can use to write code that can be run on a number of platforms, assuming you have an appropriate compiler or interpreter.
Markup Language	System of tags used to structure a document.
	not a programming language but a means of making data in a document accessible to a program
	Examples include HyperText Markup Language (HTML) and eXtensible Markup Language (XML).
Pseudocode	Writing out a program sequence using code blocks but without using the specific syntax of a particular programming language.
Interpreted Programming Languages	When you write code with an interpreted language, you do not need to compile the program

4.1 Programming language categories (cont)	
	It runs within the context of an interpreter, which converts the code into machine code at runtime.
	This means that the program probably runs more slowly but also means it is likely that you can run the program on any platform for which you have an interpreter.
	Examples of interpreted languages include scripting languages, such as JavaScript, Perl, and Python.
Query Languages	Code written in a query language, such as Structured Query Language (SQL), is designed to retrieve specific records from a dataset.
	The code does not need to be compile
Compiled Programming Languages	you must transform the code to an executable binary before it can run
	Compiling converts the source code that you wrote to machine code
	Machine code is the instructions converted to strings of ones and zeros for the CPU to process
	A compiled program generally runs quickly (compared to interpreted code). However, a compiled program tends to be platform (CPU) specific; to run on other platforms, you must recompile the source code for the new platform.
	The following languages are compiled: C++, C#, COBOL, PASCAL

4.2 Programming & interpret logic	
Program Sequence	A program is just a sequence of instructions for your computer to perform.
	In designing a program, we have to consider how input, processing, and output are all clearly defined.
Example: add two user-entered numbers together and display the sum on the screen	1 Clear the current display.
	2. Output to the screen the instructions for the operation.
	3. Ask the user for the first number
	4. Verify that the entered value is a number: a. If it is, proceed.

4.2 Programming & interpret logic (cont)

		b. If it is not, remind the user what the valid range is and prompt again.
	5. Store that number for subsequent use.	
	6. Ask the user for the second number.	
	7. Verify that the entered value is a number	a. If it is, proceed.
		b. If it is not, remind the user what the valid range is and prompt again.
	8. Store that number for subsequent use.	
	9. Retrieve the two stored numbers and add them together.	
	10. Display the result.	
Using a Flow Chart	As this restatement of the program is getting significantly more complex, it might help to visualize it. You could view the sequence as a graphical flow chart to help understand the processes.	
	With the steps shown visually in a diagram, it is easier to see that the program is not completely linear	
	here are branches and loops	
	Also notice that the program contains some duplicate steps; specifically, the verification steps and the display instructions steps	
	We can use the diagram to analyze the sequence of instructions and write better code to support that sequence.	
Pseudocode	Writing out a program sequence using code blocks but without using the specific syntax of a particular programming language.	

4.2 Programming & interpret logic (cont)		
Pseudocode keywords:	subroutines	he main routine calls some subroutines
		Each routine is completed by an "End Routine" statement
		This means (for example) when the program reaches the last step of the main routine, it closes rather than flowing through to try to execute the first subroutine.
	return	When a subroutine completes, it can return to the point in the main routine from where it was called, and the main routine continues execution
		Note that when we use structures such as this, we have to be very careful not to create infinite loops in the code by mistake.
	conditional statement/branching (IF)	There is a conditional statement (IF) that means part of the code only executes when certain conditions are true or false.
		a branch is an instruction to your computer to execute a different sequence of instructions.
	Loops	similar to branches in as much as they deviate from the initial program path according to some sort of logic condition.
		However, with a loop, you instruct your computer to perform, or repeat, a task until a condition is met.
		As well as "For" structures, loops can also be implemented by "While" statements:
	variables	store data input by the user.
	functions	(such as "sum" and "write") that we can assume are provided as features of the programming language.

4.2 Programming & interpret logic (cont)

		We don't need to code how to add two numbers together or write output to the display screen.
	user interface	the program interacts with (prompting for input and displaying output).
	comments	preceded by the ' character.
		Comments are part of the programming code that are not executed by the computer but that help the developer read and maintain the code.
	branch	this is an instruction to your computer to execute a different sequence of instructions.
Operators	Looping and branching structures depend on logical tests to determine whether to continue the loop or the branch to follow.	
	A logical test is one that resolves to a TRUE or FALSE value.	
	These tests can be performed with operators, which are used to perform arithmetic, comparison, or logical operations on variables and values.	
	Arithmetic operators include simple calculations, such as addition (+), subtraction (-), multiplication (*), division (/), etc.	

4.3 Programming concepts

basic comparison operators:	==	equal to (returns TRUE if both conditions are the same).
	!=	is not equal to.
	<	less than
	>	greater than
	<=	less than or equal to
	>=	greater than or equal to
logical operators	AND	if both conditions are TRUE, then the whole statement is TRUE.
	OR	if either condition is TRUE, then the whole statement is TRUE.

4.3 Programming concepts (cont)		
	XOR	if either condition is TRUE but not both, then the whole statement is TRUE.
	NOT	negation operator that reverses the truth value of any statement.
Identifiers	An identifier is used in a program to access a program element, such as a stored value, class, method, or interface.	
	In essence, an identifier is a label for something within your program. If your identifier stores data, then it will be either a variable or a constant.	
Variables	A variable contains a value that can change during the execution of the program. This value might be a text string, a number, or any other data type.	
	Important: Variables are usually declared, defined as a particular data type, and given an initial value at the start of the routine in which they are used. It is often possible to use undeclared variables, but this can make code harder to read and more prone to errors.	
Constants	a specific identifier that contains a value that cannot be changed within the program.	
	For example, you might want to store the numerical value for the screen dimensions or resolution.	
Container-s(Arrays,-Vectors):	a term for a special type of identifier that can reference multiple values (or elements)	
	For example, say that you want your program to store a list of user names who have logged on to the computer in the last 24 hours.	
	Arrays cannot be resized	
	Vectors can grow or shrink in size as elements are added or removed	

4.3 Programming concepts (cont)		
procedures and functions	enable you to create segments of code that you will reuse	
	function can return a value while a procedure cannot	
Attributes	values and data types that define the object.	
	The attributes are stored within the object as fields or private variables.	
	Other programs cannot access or change the fields directly.	
	They must call a particular method (see below) to do that	
Methods	defines what you can do to an object	
Properties	represent an alternative way of accessing a field publicly	
	Using a method might be regarded as quite a "heavyweight" means of doing this, so properties allow external code to ask the object to show or change the value of one of its fields.	

5.1 Database concepts/purpose		
Database	an organized collection of information.	
	The information is stored in a structured manner for easier access	
	Typically, a database consists of tables of information, organized into columns and rows.	
	Each row represents a separate record in the database, while each column represents a single field within a record.	
Usage of database	Creation	this step involves defining what information the database will store, where it will be hosted, and how it will be accessed by clients.
	Import/input	once the database has been created, it must be populated with data records.

5.1 Database concepts/purpose (cont)		
		Records can either be input and updated manually, usually using some type of form, or data might be imported from another source, or both.
	Queries	it is possible in theory to read the information in each table manually, but in order to view information efficiently, a query is used to extract it.
		A query allows the user to specify criteria to match values in one or more fields and choose which fields to display in the results so that only information of interest is selected.
	Reports	a query might return a large number of rows and be just as difficult to read as a table
		A report is a means of formatting and summarizing the records returned by a query so that the information is easy to read and interpret.
Flat File Systems	Spreadsheets and Comma Separated Values(CSV) are an example of a flat file data storage and access system rather than a database.	
Benefits of Database	Variety of data	Databases can enforce data types for each column and validate information entered as fields and records, consequently they can support a wider variety of data formats.
	Multiple concurrent users	Databases can support tens, hundreds or thousands, or even millions of users concurrently
		A single file-based data storage solution does not offer high enough speed for the volumes of transactions (adding and updating records) on enterprise-level systems.
	Scalability	able to expand usage without increasing costs at the same rate

5.1 Database concepts/purpose (cont)

		Database architecture means that extra capacity can be added later with much less investment.
		For example, in a non-scalable system, doubling the number of users would also double the costs of the system.
	Complex schemas	can manage multiple tables and link the fields in different tables to create complex schemas. In a flat file, all the information is stored within a single table.
	Speed	Databases provide access controls to protect information from unauthorized disclosure and backup/replication tools to ensure that data can be recovered within seconds of it being committed.
Storage (data persistence)	databases are often used with applications	
	While an application processes variables and other temporary data internally, this information is lost when the application is terminated.	
	A database represents a way for an application to store data persistently and securely.	

5.2 Database structures

Structured	When you store your information in a relational database, it is stored in a structured way
	enables you to more easily access the stored information and gives you flexibility over exactly what you access
	For example, you can access all fields or only certain fields. Each field has a defined data type, meaning that software that understands the database language (SQL), can parse (interpret) the content of a field easily.
Unstructured	provides no rigid formatting of the data

5.2 Database structures (cont)	
	mages and text files, Word documents and PowerPoint presentations are examples of unstructured data.
	Unstructured data is typically much easier to create than structured data.
	Documents can be added to a store simply and the data store can support a much larger variety of data types than a relational database can.
Semi-structured	Sits somewhere between structured and unstructured
	Strictly speaking, the data lacks the structure of formal database architecture
	But in addition to the raw unstructured data, there is associated information called metadata that helps identify the data.
	Email data, as well as markup languages such as XML, are forms of semi-structured data
Relational Databases	a highly structured type of database
tables	Information is organized in tables (known as relations)
fields	A table is defined with a number of fields, represented by the table columns
	Each field can be a particular data type.
row	Each row entered into the table represents a data record.
primary key	used to define the relationship between one table and another table in the database
	Each row in the table must have a unique value in the primary key field
foreign key.	When a primary key in one table is referenced in another table, then in the secondary table, that column is referred to as a foreign key.
schema	The structure of the database in terms of the fields defined in each table and the relations between primary and foreign keys

5.2 Database structures (cont)		
Constraints	It is very important that the values entered into fields are consistent with what information the field is supposed to store.	Garbage In, Garbage Out (GIGO)
	When defining the properties of each field, as well as enforcing a data type, you can impose certain constraints on the values that can be input into each field	
	A primary key is an example of a constraint. The value entered or changed in a primary key field in any given record must not be the same as any other existing record.	
	Other types of constraints might perform validation on the data that you can enter	
	Constraints can be applied at different levels. As well as applying rules to fields, they can be used at the table and schema levels too.	
Non-relational databases	sometimes referred to as “NoSQL,” which stands for Not Only SQL	
	main difference between these is how they store their information.	
	A non-relational database stores data in a non-tabular form, and tends to be more flexible than the traditional, SQL-based, relational database structures.	
	It does not follow the relational model provided by traditional relational database management systems.	
key–value database	a data storage paradigm designed for storing, retrieving, and managing associative arrays, and a data structure more commonly known today as a dictionary or hash table	
	Dictionaries contain a collection of objects, or records, which in turn have many different fields within them, each containing data.	

5.2 Database structures (cont)

	hese records are stored and retrieved using a key that uniquely identifies the record, and is used to find the data within the database.
Document databases	a type of nonrelational database that is designed to store and query data as JSON-like documents
	make it easier for developers to store and query data in a database by using the same document-model format they use in their application code.

5.3 Database Interface Methods

Relational Methods	Database interfaces are the processes used to add/update information to and extract (or view) information from the database
	In an RDBMS, the use of Structured Query Language (SQL) relational methods is critical to creating and updating the database
Data Definition Methods:	Data Definition Language (DDL) commands refer to SQL commands that add to or modify the structure of the database.
CREATE	this command can be used to add a new database on the RDBMS server (CREATE DATABASE) or to add a new table within an existing database (CREATE TABLE).
	The primary key and foreign key can be specified as part of the table definition
Alter Table	This allows you to add, remove (drop), and modify table columns (fields), change a primary key and/or foreign key, and configure other constraints.
	There is also an ALTER DATABASE command, used for modifying properties of the whole database, such as its character set.
DROP	used to delete a table (DROP TABLE) or database (DROP DATABASE).
	Obviously, this also deletes any records and data stored in the object.
CREATE INDEX	specifying that a column (or combination of columns) is indexed speeds up queries on that column.

5.3 Database Interface Methods (cont)

	The tradeoff is that updates are slowed down slightly (if the column is not suitable for indexing, updates may be slowed down quite a lot.
	The DROP INDEX command can be used to remove an index.
INSERT INTO TableName	adds a new row in a table in the database.
UPDATE TableName	changes the value of one or more table columns.
	This can be used with a WHERE statement to filter the records that will be updated
	If no WHERE statement is specified, the command applies to all the records in the table.
DELETE FROM TableName	—deletes records from the table
	As with UPDATE, this will delete all records unless a WHERE statement is specified.
SELECT	enables you to define a query to retrieve data from a database.
Permissions:	SQL supports a secure access control system where specific user accounts can be granted rights over different objects in the database (tables, columns, and views for instance) and the database itself.
	When an account creates an object, it becomes the owner of that object, with complete control over it.
	The owner cannot be denied permission over the object
	The owner can be changed however, using the ALTER AUTHORIZATION statement.
Database Access Methods:	Database access methods are the processes by which a user might run SQL commands on the database server or update or extract information using a form or application that encapsulates the SQL commands as graphical controls or tools.
Direct/Manual Access:	Administrators might use an administrative tool, such as phpMyAdmin, to connect and sign in to an RDBMS database.
	Once they have connected, they can run SQL commands to create new databases on the system and interact with stored data.

5.3 Database Interface Methods (cont)

	This can be described as direct or manual access.
Query/Report Builder	There are many users who may need to interact closely with the database but do not want to learn SQL syntax
	A query or report builder provides a GUI for users to select actions to perform on the database and converts those selections to the SQL statements that will be executed
Programmatic Access	A software application can interact with the database either using SQL commands or using SQL commands stored as procedures in the database.
	Most programming languages include libraries to provide default code for connecting to a database and executing queries.
User Interface/Utility Access:	:An application might use a database in the background without the user really being aware of its presence.
	Alternatively, the application might prov dinary users to add and search records.
Backups and Data Expor	As with any type of data, it is vital to make secure backups of databases.
	Most RDBMS provide stored procedures that invoke the BACKUP and RESTORE commands at a database or table level.
	It may also be necessary to export data from the database for use in another database or in another type of program, such as a spreadsheet.
Database dump	A dump is a copy of the database or table schema along with the records expressed as SQL statements.
	These SQL statements can be executed on another database to import the information.
Exporting	Most database engines support exporting data in tables to other file formats, such as Comma Separated Values (.CSV) or native MS Excel (.XLS)

6.1 confidentiality/integrity/availability

Confidentiality concerns	Security is the practice of controlling access to something

6.1 confidentiality/integrity/availability (cont)

	Security must be balanced against accessibility: if a system is completely secure, then no one has access to it, and it is unusable.	
Confidentiality	the information should only be known to authorized users.	
Integrity	the information is stored and transferred as intended and that any modification is authorized.	
Availiability	the information is accessible to those authorized to view or modify it.	
Security Threats- Confidentiality Concerns	Confidentiality means that information is only revealed to authorized people. This can be compromised in a number of ways:	
	Snooping	this is any attempt to get access to information on a host or storage device (data at rest) that you are not authorized to view
		An attacker might steal a password or find an unlocked workstation with a logged-on user account, or they might install some sort of spyware on the host.
	Eavesdropping/wiretapping	this is snooping on data or telephone conversations as they pass over the network.
		Snooping on traffic passing over a network is also often called sniffing.
		It can be relatively easy for an attacker to "tap" a wired network or intercept unencrypted wireless transmissions
		Networks can use segmentation and encryption to protect data in-transit.

6.1 confidentiality/integrity/availability (cont)		
	Social engineering/dumpster diving	this means getting users to reveal information or finding printed information.
Integrity Concerns	Integrity means that the data being stored and transferred has not been altered without authorization.	
	Some threats to integrity include the following attacks:	
	On Path attack	where a host sits between two communicating nodes, and transparently monitors, captures, and relays all communications between them.
	Replay	where a host captures another host's response to some server and replays that response in an effort to gain unauthorized access.
		Replay attacks often involve exploiting an access token generated by an application
	Impersonation	—a common attack is where a person will attempt to figure out a password or other credentials to gain access to a host.
Availability Concerns	Availability means keeping a service running so that authorized users can access and process data whenever necessary.	
	Availability is often threatened by accidents and oversights as well as active attacks.	
	Denial of Service (DoS	—this is any situation where an attacker targets the availability of a service.
		A DoS attack might tamper with a system or try to overload it in some way.
	Power outage	if you lose power, then clearly your computers cannot run.
		Using standby power can help mitigate this issue

6.1 confidentiality/integrity/availability (cont)	
	Using an Uninterruptible Power Supply (UPS) can provide a means to safely close down a server if building power is interrupted.
Hardware failure	if a component in a server fails, then the server often fails
	A hard disk contains moving parts and will eventually fail
	If a disk fails, you will likely lose access to the data on the failed disk and quite possibly lose the data.
	You can compensate against hardware failure by provisioning redundant components and servers. The service is then config
Destruction	the loss of a service or data through destruction can occur for a number of reasons.
	At one extreme, you might lose a data center through a fire or even an act of terrorism.
	Either way, putting your servers in a physically secure room and controlling access to that room can help protect against these issues.
Service outage	any of the situations above can lead to service unavailability.
	Many organizations use online, cloud-based apps and services these days
	You need to consider how third-party service failures may affect your data processing systems.
	When you decide which cloud provider to use, consider the options they provide for service availability and fault tolerance.

6.1 confidentiality/integrity/availability (cont)		
Authentication, Authorization, and Accounting	To guard against these threats to confidentiality and integrity, data and data processing systems are protected by access controls	
	An access control system normally consists of one or more of the following types of controls:	
	Authentication	means one or more methods of proving that a user is who they say they are and associates that person with a unique computer or network user account.
	Authorization	means creating one or more barriers around the resource such that only authenticated users can gain access
		Each resource has a permissions list specifying what users can do.
		Resources often have different access levels, for example, being able to read a file or being able to read and edit it
	Accounting	means recording when and by whom a resource was accessed.

6.2 Device security/best practices	
Host Firewall	A firewall restricts access to a computer or network to a defined list of hosts and applications.
	Basic packet filtering firewalls work on the basis of filtering network data packets as they try to pass into or out of the machine.
Windows Defender Firewall	it is enabled on all network connections by default unless it has been replaced by a third-party firewall.
Safe Browsing Practice	Using Free/Open Networks can be intercepted by anyone else connected to the network and by the person that owns the network.

6.2 Device security/best practices (cont)		
	To mitigate this, use a security-enabled protocol (SSL/TLS) that encrypts the link between your client and the web or mail server.	
Device hardening	refers to a set of policies that make mobile and workstation computers and network appliances more secure	
	many options for hardening mobile devices, configuring a screen lock out and encrypting data for instance, were discussed earlier.	
Hardening policies	Anti-virus/a-nti-malware	malware is software that aims to damage a computer or steal information from it.
		malware is software that aims to damage a computer or steal information from it.
	Patching/-updates	OS files, driver software, and firmware may be exploitable by malware in the same way as applications software.
		It is important to keep computers and other devices configured with up-to-date patches and firmware
	Enabling passwords	most operating systems allow the use of an account without a password, PIN, or screen lock, but this does not mean it is a good idea to do so
		All computing devices should be protected by requiring the user to input credentials to gain access.
	Default/weak passwords	network devices such as wireless access points, switches, and routers ship with a default management password, such as "password," "admin," or the device vendor's name
		These should be changed on installation.
		the password used should be a strong one—most devices do not enforce complexity rules so the onus is on the user to choose something secure.

6.2 Device security/best practices (cont)		
	Disabling unused features	any features, services, or network protocols that are not used should be disabled.
		This reduces the attack surface of a network device or OS.
		Attack surface means the range of things that an attacker could possibly exploit in order to compromise the device.
	Removing unwanted/unnecessary software	new computers ship with a large amount of pre-installed software, often referred to as bloatware.
		These applications should be removed if they are not going to be used
Device use best practices	When installing new software applications or drivers, it is important to obtain the setup files from a legitimate source.	
Reputable sources include	Vendor app stores (for example, Windows Store, Google Play Store, Apple App Store).	
	Merchant app stores, such as Amazon Appstore.	
	Authorized resellers, Original Equipment Manufacturer (OEM) vendors, and managed service providers. If in any doubt, check the reseller or OEM's accreditation	
Third Party Sites	If you need to use a driver from a site such as this, try to research it as much as you can.	
	Search for references to the site on the web to find out if anyone has posted warnings about it.	
	If you trust this site, check for a forum where other users might have tried a specific driver package and indicated whether it is legitimate or not	
	Check that it is protected by a valid digital certificate and that its downloaded over a secure HTTPS connections.	

6.3 Behaviour security concepts	
Expectations of privacy:	type of privacy consideration should also affect your choice of Internet Service Provider (ISP) and web search engine

6.3 Behaviour security concepts (cont)

	Your browsing and search history reveal an enormous amount of very personal information	
	While the actual content of what you view or send to a site might be protected by encryption, the URL or web address of the site is not	
	Privacy issues do not just affect websites, social media sites, ISPs, and search providers. It is also possible that this type of data will be collected from mobile apps and desktop software. It is typical for software such as Windows or Office to prompt you to allow usage and troubleshooting data to be sent back to the vendor (Microsoft) for analysis for example.	
Written Policies and Procedures	As a vital component of a company's IT infrastructure, employees must understand how to use computers and networked services securely and safely and be aware of their responsibilities	
	To support this, the organization needs to create written policies and procedures to help staff understand and fulfill their responsibilities and follow best practices	
	The value of a comprehensive policy is that it removes any uncertainty that employees may have about what to do in a given situation.	
Handling Confidential Information:	Passwords	Users must keep their work passwords known only to themselves.

6.3 Behaviour security concepts (cont)

	This means not writing down the password, not telling it to anyone else, and not using it to authenticate to any other services or websites.
Personally Identifiable Information (PII	The rise in consciousness of identity theft as a serious crime and growing threat means that there is an increasing impetus on government, educational, and commercial organizations to take steps to obtain, store, and process Personally Identifiable Information (PII) more sensitively and securely.
	Staff should be trained to identify PII and to handle personal or sensitive data appropriately.
	This means not making unauthorized copies or allowing the data to be seen or captured by any unauthorized people
Company Confidential Information	Any of the business information used to run a company could be misused in the wrong hands
	This sort of information includes product designs or plans, marketing plans, contracts, procedures and workflows, diagrams and schematics, and financial information.
	This information must not be disclosed to unauthorized people and should always be stored on media that are subject to network access controls and/or encrypted.
	Paper or electronic copies of this sort of information that are no longer needed should be destroyed rather than discarded

6.4 AAA & non-repudiation

AAA	Authentication, Authorization, and Accounting - the principal stages of security control. A resource should be protected by all three types of controls

6.4 AAA & non-repudiation (cont)

Accounting	The accounting part of the access control system provides an audit log of how users have authenticated to the network and used their access privileges	
	Accounting is usually provided for by logging events.	
	Accounting is an important part of ensuring non-repudiation	
Non Repudiation	the principle that the user cannot deny having performed some action. Apart from logging, several mechanisms can be used to provide non-repudiation:	
	Video	surveillance cameras can record who goes in or out of a particular area.
	Biometrics	strong authentication can prove that a person was genuinely operating their user account and that an intruder had not hijacked the account.
	Signature	similarly, a physical or digital signature can prove that the user was an author of a document (they cannot deny writing it)
	Receipt	issuing a token or receipt with respect to some product or service is proof that a user requested that product and that it was delivered in a timely manner.
Multifactor Authentication	Strong authentication is multi-factor	
	r. Authentication schemes work on the basis of something you know, something you have, or something you are.	

6.4 AAA & non-repudiation (cont)

	These schemes can be made stronger by combining them (for example, protecting use of a smart card certification [something you have] with a PIN [something you know]).
PIN (Personal Identification Number)	Number used in conjunction with authentication devices such as smart cards; as the PIN should be known only to the user, loss of the smart card should not represent a security risk.
Token	A token contains some sort of authentication data. Software tokens are generated by logon systems, such as Kerberos, so that users do not have to authenticate multiple times (Single Sign-on).
	A hardware token can be a device containing a chip with a digital certificate but is more usually a device that generates a one-time password.
	This can be used in conjunction with an ordinary user name and password (or PIN) to provide more secure two-factor authentication
Permissions	To access files and folders on a volume, the administrator of the computer will need to grant file permissions to the user (or a group to which the user belongs). File permissions are Page 9/16 supported by NTFS-based Windows systems
Access Control	Creating one or more barriers around a resource such that only authenticated users can gain access.

6.4 AAA & non-repudiation (cont)	
	Each resource has an Access Control List (ACL) specifying what users can do. Resources often have different access levels (for example, being able to read a file or being able to read and edit it).
ACL (Access Control List)	The permissions attached to or configured on a network resource, such as folder, file, or firewall. The ACL specifies which subjects (user accounts, host IP addresses, and so on) are allowed or denied access and the privileges given over the object (read only, read/write, and so on).
Least Privilege	Least privilege is a basic principle of security stating that something should be allocated the minimum necessary rights, privileges, or information to perform its role
User Account	Each user who wishes to access a Windows computer will need a logon ID, referred to as a user account
	Each user will normally have a local profile, containing settings and usercreated files. Profiles are stored in the "Users" folder
Group Account	A group account is a collection of user accounts. These are useful when establishing file permissions and user rights because when many individuals need the same level of access, a Page 15/16 group could be established containing all the relevant users. The group could then be assigned the necessary rights

6.4 AAA & non-repudiation (cont)

MAC (Mandatory Access Control)	Access control model where resources are protected by inflexible, system defined rules. Resources (objects) and users (subjects) are allocated a clearance level (or label)
	There are a number of privilege models, such as Bell-LaPadula, Biba, and Clark-Wilson providing either confidentiality or integrity.
DAC (Discretionary Access Control)	Access control model where each resource is protected by an Access Control List (ACL) managed by the resource's owner (or owners).

6.5 Password best practices

Length	a longer password is more secure. Around 9–12 characters is suitable for an ordinary user account
	Administrative accounts should have longer passwords (14 or more characters).
Complexity	improve the security of a password
	No single words—better to use word and number/punctuation combinations, no obvious phrases etc.
Memorability	artificial complexity makes a password hard to remember, meaning users write them down or have to reset them often
	Use longer phrases etc.
Maintain confidentiality	do not write down a password or share it with other users.
History/expiration	change the password periodically
	Many systems can automatically enforce password expiration, meaning users have to choose a new password.
Reuse across Sites	Users must be trained to practice good password management, or at the very least not to re-use work passwords for web accounts.
password reset	allows a user who has forgotten a password to self-select a new one.

6.6 Encryption

Encryption	an ancient technique for hiding information

6.6 Encryption (cont)	
	Someone obtaining an encrypted document, or cipher text, cannot understand that information unless they possess a key.
Plain text (or clear text	this is an unencrypted message.
Cipher text	an encrypted message.
Cipher	this is the process (or algorithm) used to encrypt and decrypt a message
Data States	Data can be described as being at rest or in transit
Data at rest	this state means that the data is in some sort of persistent storage media.
	In this state, it is usually possible to encrypt the data using techniques such as whole disk encryption, mobile device encryption, database encryption, and file- or folder-level encryption.
File-level encryption	useful as a method on large-volume storage devices
Disk encryption	sometimes used in conjunction with filesystem-level encryption with the intention of providing a more secure implement-ation
	generally uses the same key for encrypting the whole drive, all of the data can be decrypted when the system runs
	However, some disk encryption solutions use multiple keys for encrypting different volumes.
Mobile devices	smartphones and tablets have encryption options that will also provide protection of storage.
	it’s not typically a disk but is still just storage that’s encrypted and accessed using some key
Data in transit (or data in motion)	this is the state when data is transmitted over a network, such as communicating with a web page via HTTPS or sending an email
	In this state, data can be protected by a transport encryption protocol, such as Secure Sockets Layer (SSL)/Transport Layer Security (TLS).
Virtual Private Network (VPN)	connects the components and resources of two private networks over another public network or connects a remote host with an Internet connection to a private local network.
	A VPN is a "tunnel" through the Internet or any other network.

6.6 Encryption (cont)	
Email encryption	encryption of email messages to protect the content from being read by entities other than the intended recipients
	may also include authentication.
	Email is prone to the disclosure of informatio
	Most emails are currently transmitted in the clear form
	All emails sent using Gmail or Outlook are encrypted by default.
Hypertext Transfer Protocol Secure (HTTPS)	provides for encrypted transfers, using SSL and port 443.

6.7 Business continuity	
Business Continuity Plan (BCP)/-Continuity of Operations Plan (COOP)	A business continuity plan is designed to ensure that critical business functions demonstrate high availability and fault tolerance.
	Typically, this is achieved by allowing for redundancy in specifying resources.
	Examples include cluster services, RAID disk arrays, UPS. Business continuity plans should not be limited to technical elements however; they should also consider employees, utilities, suppliers, and customers.
	Associated with business continuity is the disaster recovery plan, which sets out actions and responsibilities for foreseen and unforeseen critical incidents.
	e vulnerabilities can be mitigated by creating contingency plans and resources that allow the system to be resilient to failures and unexpected outage
	Most contingency plans depend on providing redundancy at both the component and system leve
	If a component or system is not available, redundancy means that the service can failover to the backup either seamlessly or with minimum interruption.
Fault Tolerance	protect against losing access to a computer system when a component fails
	systems that contain additional components to help avoid single points of failure
Data Redundancy	Combining hard disks into an array of disks can help to avoid service unavailability due to one or more disks failing.

6.7 Business continuity (cont)	
Redundant Array of Independent Disks (RAID) standard	evolved to offer a variety of fault tolerant solutions. Different RAID solutions are defined in numbered levels.
Network Redundancy	Without a network connection, a server is not of much use
	As network cards are cheap, it is commonplace for a server to have multiple cards (adapter fault tolerance)
	Multiple adapters can be configured to work together (adapter teaming)
	This provides fault tolerance—if one adapter fails, the network connection will not be lost—and can also provide load balancing (connections can be spread between the cards).
	Network cabling should be designed to allow for multiple paths between the various servers, so that during a failure of one part of the network, the rest remains operational (redundant connections)
	Routers are great fault tolerant devices, because they can communicate system failures and IP packets can be routed via an alternate device
Power Redundancy	means deploying systems to ensure that equipment is protected against these events and that network operations can either continue uninterrupted or be recovered quickly.
Replication	between multiple data centers to guard against risks
	Replication is the process of synchronizing data between servers and potentially between sites.
	This replication might be real-time or bundled into batches for periodic synchronization.
Disaster Recovery	creates workflows and resources to use when a specific disaster scenario affects the organization
	A disaster could be anything from a loss of power or failure of a minor component to man-made or natural disasters.
	For each high-risk scenario, the organization should develop a plan identifying tasks, resources, and responsibilities for responding to the disaster

6.7 Business continuity (cont)	
Prioritiz-ation	disaster recovery plans should identify priorities for restoring particular systems first
	This process has to be conditioned by dependencies between different systems.
	The servers running the website front-end might not be able to operate effectively if the servers running the database are not available
Data Restor-ation	If a system goes down, there may be data loss
	Data can either be restored from backup or by switching over to another system to which data has been replicated. It is vital that the integrity of the data be checked before user access is re-enabled.
Restoring Access	Once the integrity of the failover or restored system has been verified, you can re-enable user access and start processing transa-ctions again.

By **Bayan** (Bayan.A)
cheatography.com/bayan-a/

Published 15th December, 2022.
Last updated 9th December, 2022.