**COMPUTERS AND COMPUTING SYSTEMS, NQF LEVEL 4, CREDITS 12**

**LEARNER WORKBOOK**

|  |  |
| --- | --- |
| **Module #** | 251201-005-00-KM-01: |
| **NQF Level** | level 4 |
| **Notional hours** | 120 |
| **Credit(s)** | Cr 12 |
| **Occupational Code** | 251201005 |
| **SAQA QUAL ID** |  |
| **Qualification Title** | Occupational Certificate: Software Developer |

**CONTACT INFORMATION:**

|  |  |
| --- | --- |
| **Name** |  |
| **Contact Address** |  |
| **Telephone (H)** |  |
| **Telephone (W)** |  |
| **Cellular** |  |

**Note to the learner**

This Learner Guide provides a comprehensive overview of the module. It is designed to improve the skills and knowledge of learners, and thus enabling them to effectively and efficiently complete specific tasks.

**Purpose**

The main focus of the learning in this knowledge module is to build an understanding of what computers can do and the processes that make them function in terms of the four major parts: input, output, CPU (central processing unit) and memory. It gives an overview of networks and connectivity as well as security issues pertaining to IT ecosystems

**Topic elements to be covered include**

The learning will enable learners to demonstrate an understanding of:

* KM-01-KT01: Problem solving skills for IT Professionals 5%
* KM-01-KT02: Techniques for safety 5%
* KM-01-KT03: System components 5%
* KM-01-KT04: Motherboards 5%
* KM-01-KT05: Processors 5%
* KM-01-KT06: Memory 5%
* KM-01-KT07: BIOS and CMOS 5%
* KM-01-KT08: Hard drives and storage devices 5%
* KM-01-KT09: Power supplies and voltage 5%
* KM-01-KT10: Ports, cables, and connectors 2%
* KM-01-KT11: Networking and network operating systems 5%
* KM-01-KT12: Networking and wireless connections 3%
* KM-01-KT13: Input and output devices 3%
* KM-01-KT14: Installing and managing printers 2%
* KM-01-KT15: Mobile devices, multimedia, and laptop computers 2%
* KM-01-KT16: Preventative maintenance 2%
* KM-01-KT17: Troubleshooting procedures 2%
* KM-01-KT18: Operating systems 5%
* KM-01-KT19: Managing files 2%
* KM-01-KT20: Applications utility, troubleshooting, and optimization 2%
* KM-01-KT21: Configuring device drivers 5%
* KM-01-KT22: Recovery 5%
* KM-01-KT23: Cloud computing 5%
* KM-01-KT24: Security fundamentals 5%
* KM-01-KT25: Programming and development 5%

**Entry Requirements**

NQF 4

**Provider Accreditation Requirements for the Knowledge Module**

**Physical Requirements:**

* The provider must have lesson plans and structured learning material or provide learners with access to structured learning material that addresses all the topics in all the knowledge modules as well as the applied knowledge in the practical skills
* QCTO/ MICT SETA requirements

**Human Resource Requirements:**

* Lecturer/learner ratio of 1:20 (Maximum)
* Qualification of lecturer (SME):
* NQF 6 in industry recognised qualifications with 1 year’s experience in the IT industry
* AI vendor certification (where applicable)
* Assessors and moderators: accredited by the MICT SETA

**Legal Requirements:**

* Legal (product) licences to use the software for learning and training (where applicable)
* OHS compliance certificate
* Ethical clearance (where necessary)

**Exemptions**

* No exemptions, but the module can be achieved in full through a normal RPL process

**Venue, Date and Time:**

Consult your facilitator should there be any changes to the venue, date and/or time.

Refer to your timetable

**Assessments**

The only way to establish whether you are competent and have accomplished the learning outcomes is through continuous assessments. This assessment process involves interpreting evidence about your ability to perform certain tasks. You will be required to perform certain procedures and tasks during the training programmer and will be assessed on them to certify your competence.

This module includes assessments in the form of self-evaluations/activities and exercises. The exercises, activities and self-assessments will be done in pairs, groups or on your own. These exercises/activities or self-assessments (Learner workbook) must be handed to the facilitator. It will be added to your portfolio of evidence, which will be proof signed by your facilitator that you have successfully performed these tasks.

Listen carefully to the instructions of the facilitator and do the given activities in the time given to you.

# SECTION 1: KM-01-KT01: Problem solving skills for IT Professionals 5%

**Problem-solving steps and the application thereof are explained**

**Identification of the problem**

Identifying a problem in IT involves the process of finding the exact cause of a problem inside a system by comparing what is seen to established patterns until a match is found, allowing for effective remedy of the underlying problem.

Establishing a probable cause

This step requires substantial research, which includes source documentation, internal reports, and Google searches. It could involve questioning the obvious and looking into alternative solutions, such as top-to-bottom or bottom-to-top for stacked technology. Newer troubleshooters frequently struggle to avoid challenging the obvious, therefore extensive notes, including website data, online URLs, and team member comments, are critical.

Testing to determine the cause

Software testing is a critical process for identifying and correcting problems in real-world scenarios. Undefined quality standards, duplicate test environments, a lack of communication, unstable environments, and poor requirements collection are all significant issues. Testers may struggle to satisfy client needs, meet quality requirements, and comply with regulations if quality standards are unclear. To address these issues, teams should establish quality standards upfront, implement a realistic test environment, and invest in current collaboration tools.

Another difficulty is a lack of communication, as testers frequently work alone and rarely interact with other team members. This might result in a lack of understanding of risks and concerns, posing a challenge to the project. To address these difficulties, formalising test environment requirements early in the testing process can assist capture needs on time, provide appropriate resources, and construct new environments.

Inadequate requirements collection can potentially interrupt the testing process, resulting in insufficient functionality or the discovery of additional requirements later in the development lifecycle. Proper collection ensures that teams understand what features the product should include, the level of functionality required, and the relevant faults and issues.

To make testing a more streamlined and challenge-free process, teams should collaborate with partners who can apply strategies that help overcome problems while meeting quality and cost objectives. By addressing these issues, testing can become a more efficient and effective method for producing high-quality products.

**Establishing a plan to resolve the problem**

In this stage first create a plan of action and seek clearance from other IT personnel/people involved in the project.

Consider the following: downtime, software downloads, staging environment testing, documentation, data backup, and approval. After completing this stage, put the solution into action by running scripts, updating systems, altering configuration files, and adjusting firewall settings. Prepare a rollback plan in case the fix does not resolve the problem. Implementing the recommended fix may be faster than the research phases, but research is required to address the root cause and reduce downtime.

Implementing your solution

The plan of action for implimantation includes supervised and monitored action to guarantee proper implementation and corrective action. This procedure enables efficient task execution, identifies progress, and determines appropriate actions. Reviewing progress indicates the strategy's success, and significant differences require plan adjustment. Corrective action may include either planned countermeasures or unexpected efforts to handle unforeseen problems. Minor issues may not warrant intervention, whereas serious flaws may demand abandonment. These steps must continue until the plan is finalised.

Verifying functionality

Barry Boehm's concept of Static Testing and Validation emphasizes the importance of ensuring a software system meets specifications and standards. Static Testing involves inspections, reviews, walkthroughs, and desk-checking, while Validation is the process of ensuring the product meets high-level requirements. Both methods involve activities like black box, white box, unit testing, and integration testing to ensure the product meets the required purpose.

Implementing preventative measures

Home computers are vulnerable to cyber threats, so it's crucial to install antivirus software, keep it updated, create an emergency boot disk, regularly backup files, configure strict security settings, avoid unknown programs, disable hidden filename extensions, and disconnect from the internet.

Documenting results

A software test document is an essential tracking tool for software development projects, especially those without a dedicated QA specialist. It follows three principles: logic, coherence, and structure. Test cases are critical for structuring testing methodologies, raising coverage metrics, recording current conditions, encouraging communication, storing data, doing regression, and enhancing test requirement quality. Each test case is dynamic and can fail or succeed, assisting software testing efforts while not burdening the project.

Software testers assign 'Created' to new test cases, which can be moved to 'Planned', 'Not Tested', 'Work in progress', or 'Skipped' depending on complexity. There are three phases: 'Failed', 'Passed', and 'Blocked'. Test suits determine the order of testing, and errors in test documents can lead to misinterpretations and misunderstandings. To avoid errors, testers should make test cases concise, avoid repetition, use correct tenses, and avoid grammar mistakes.

# SECTION 2: KM-01-KT02 : Techniques for safety 5%

**Describe the OSHA electrical safety standard 1926.431**

Electrical safety precautions are crucial for workers to avoid injuries or fatalities. Employers should label circuits with easy-to-spot signage, warn employees before starting work in areas with live circuits, and regularly locate and inspect circuits.

To prevent accidents, employees should be trained in proper safety techniques and precautions. Some generalized tips include:

1. Draft a project plan beforehand to assess the equipment and environment to spot potential hazards. This will ensure that workers use the proper PPE and IPE during the job and know where the correct circuit is for shutting off power.

2. Wear the right clothing and gear, such as rubber gloves, insulating sleeves, and safety glasses. Fire-resistant clothing can also help prevent injury due to their non-conductive fibers or flame-retardant treatment. Both employers and employees should determine if additional PPE is necessary and avoid wearing metal, such as watches or jewelry.

3. Use the Buddy System to ensure that someone can call for help if necessary or perform CPR. Both individuals should be trained in electrical safety and CPR before starting work.

4. Use the Lock Out Tag Out (LOTO) System to ensure that all circuits are shut off and de-energized before working. The system has six steps: inspect the system, shut down the circuit, isolate the equipment, lock and tag any switches or buttons that can turn the equipment on, check for stored energy, and verify everything.

5. Avoid working in wet areas, as water is a potent electrical conductor, and workers must address standing water or cover it with non-conductive material.

6. Use a Ground Fault Circuit Interrupter (GFCI) as a last resort. GFCIs are portable devices that can detect power surges and kill power automatically, acting as a final failsafe in case of an accident.

7. Stay away from overhead power lines, as many injuries and accidents occur due to overhead lines. Workers should be hyper-aware of overhead lines and inspect power cords and outlets for damage.

# SECTION 3: KM-01-KT03 : System components 5%

**Various types of system components are identified and described**

System Components are what makes the computer function, basically operate input process it and give out an output. System Components consists of hardware and software parts integrated to perform complex tasks.

Hardware components consist of the central processing unit (CPU), random access memory (RAM), Storage, Motherboard, power supply unit (PSU), Graphical Processing Unit (GPU), cooling systems, Input Devices, Output Devices and Network Components.

Software Components consists of Operating System, Devices Drivers, Firmware, Application Software and Utilities.

**Hardware components and their functionalities:**

* Central Processing Unit (CPU) is the brain of the computer that performs most calculations. Carry out instructions from programs.
* Memory (RAM): Random Access Memory (RAM) temporarily stores data and instructions needed by the CPU to accomplish operations. Volatile memory: data is lost when the machine is turned off.
* Storage exists as Hard Disc Drive (HDD) is a traditional storage device with spinning discs for reading and writing data, and Solid State Drive (SSD) is a faster storage device that stores data in flash memory.
* Motherboard is the main circuit board that houses the CPU, RAM, and other components. Provides connectors for additional components and peripherals.
* Power Supply Unit (PSU) converts electrical power from an outlet to a usable form for computers and provides power for the motherboard and other components.
* Graphics Processing Unit (GPU) renders images, videos, and animations and can be built into the CPU or used as a separate dedicated card.
* Cooling Systems generally consists of Fans that provides basic air cooling, Heat Sinks are metal structures that dissipate heat ,and Liquid Cooling Systems which use liquid to remove heat from components.
* Input Devices provides users with the ability to give instruction to the computer. The generally used ones consist of Keyboard which is used for text input, a Mouse that is used to point and click on content, and a touchscreen that enables touch input.
* Output Devices are used by the computer to output what has been processed by computing system. The most commonly used are a Monitor which shows visual results on a screen, printers create physical copies of documents, and Speakers produce sound.
* Networking Components are component that serves a specific purpose in connecting devices and assuring data flow throughout a network to and from the computer. Network Interface Card (NIC) links the computer to a network and Modems/Routers allows you to connect to the internet and manage network traffic.

**Software Components and their functionalities:**

# SECTION 4: KM-01-KT04 : Motherboards 5%

**Understanding of motherboards, primary components and related aspects is demonstrated**

The motherboard is a large, printed circuit board (PCB) that contains and connects many of the computer's critical parts, such as the CPU, memory, and external connected memory devices. It is sometimes referred to as the mainboard or logic board.

The motherboard, also known as the mainboard or logic board (in Apple devices), is a large printed circuit board (PCB) that holds and connects most of the crucial components of a computer, including the CPU, memory, and expansion cards.

Primary Components of a Motherboard

* The central processing unit (CPU) of a motherboard is housed in a CPU socket, of which the type varies depending on the CPU manufacturer. The data flow between the CPU, RAM, and peripheral devices is controlled by a collection of integrated circuits called a chipset, which is usually split into two sections: the southbridge for slower connections and the northbridge for faster connections. A motherboard's memory slots (also known as DIMM slots) might have different numbers installed in different types of RAM.
* GPUs, sound cards, network cards, and other expansion cards can be added using expansion slots. The most popular type of expansion slot, PCI Express (PCIe) slots are mostly utilized by graphics cards. It is possible that older motherboards have legacy slots.
* SATA ports are used to connect optical drives, high-speed SSDs, and hard drives. M.2 slots are used to connect SSDs, and NVMe support is used to connect NVMe drives. The 24-pin ATX Connector, the 8-pin/4-pin CPU Power Connector, and extra power connectors for stability during overclocking are examples of power connectors.
* The firmware required to start the computer and control hardware settings is stored on the BIOS/UEFI Chip. The Basic Input/Output System, or BIOS, is the conventional interface; in contrast, UEFI provides a more user-friendly interface and compatibility for larger hard drives.
* External devices such as USB, HDMI, DisplayPort, VGA, or DVI, Ethernet, audio jacks, and PS/2 connections are connected to the back I/O Panel. Fans, front panel ports, and other internal parts are connected by internal connectors.
* Voltage Regulator Modules (VRMs) maintain a steady and uniform voltage by controlling and supplying power to the CPU. Fan headers, heatsinks, and water cooling assistance are examples of cooling solutions.

# SECTION 5: KM-01-KT05 : Processors 5%

**Understanding of processers and related aspects is demonstrated**

**The majority of a computer's calculations are performed by the processor, often known as the central processing unit (CPU). It handles data flow to and from other areas of the computer, carries out arithmetic and logic operations, and carries out commands from programs. The majority of commands from the computer's hardware and software are interpreted and carried out by the CPU, which is an essential part of every computing system. A single modern CPU chip has billions of transistors, making them extremely complicated devices.**

**CPU Functions**

• Control Unit (CU): Directs processor operation, fetches instructions, decodes, and executes them.

• Arithmetic Logic Unit (ALU): Performs arithmetic and logical operations.

• Registers: Small, fast storage locations within the CPU.

• Cache Memory: Stores frequently accessed data and instructions to speed up processing.

• Organized in multiple levels (L1, L2, L3).

**CPU Performance Factors**

• Clock Speed: Measured in GHz, indicates how many cycles per second the CPU can execute. Higher clock speeds generally mean faster processing.

• Cores: Modern CPUs have multiple cores, each processing its own thread of instructions. This improves performance for multithreaded applications and multitasking.

• Threads: Sequences of instructions that the CPU can execute. Hyper-threading technology allows a single core to manage multiple threads.

• Instruction Set Architecture (ISA): Defines the set of instructions a CPU can execute. Examples include x86, ARM, and RISC-V.

• Pipelining: Technique to execute multiple instructions simultaneously, increasing the CPU's instruction throughput.

**Types of Processors**

* General-Purpose Processors: Used in desktops, laptops, servers. Examples include Intel Core and AMD Ryzen.
* Mobile Processors: Designed for smartphones and tablets. Examples include Apple A-series and Qualcomm Snapdragon.
* Embedded Processors: Used in embedded systems like automotive control, home appliances, and industrial machines. Examples include ARM Cortex-M series.
* Graphics Processing Units (GPUs): Specialized processors for graphics and parallel processing tasks. Examples include NVIDIA GeForce and AMD Radeon.
* Server and Workstation Processors: Designed for high-performance computing tasks, servers, and professional workstations.

**CPU Performance Factors**

* Clock Speed: Higher speeds generally improve performance, but efficiency and thermal constraints must be considered.
* Core Count: More cores can enhance performance in multithreaded applications and multitasking environments.
* Cache Size: Larger cache sizes reduce time needed to access frequently used data and instructions.
* Thermal Design Power (TDP): Indicates the maximum amount of heat the CPU can generate, influencing cooling requirements and energy consumption.
* Manufacturing Process: Smaller processes allow for more transistors on a chip, improving performance and efficiency.

**Overclocking:** Increases the clock speed and voltage beyond manufacturer's specifications for higher performance, requiring robust cooling solutions.

**Integrated vs. Discrete Graphics:** Built-in graphics suitable for general computing tasks and light gaming.

# SECTION 6: KM-01-KT06 : Memory 5%

**Purpose of memory and how it relates to computer components is described**

A computer system's memory is an essential component that stores data and instructions that the CPU needs for retrieval fast. It performs a few functions, such as data caching, buffering, multitasking, program execution, and temporary data storage. RAM allows for speedy read and write access to the data that the CPU needs for processing, allowing for quick retrieval and storing. A program is loaded into RAM during operation from long-term storage, enabling real-time operation. Memory serves as a buffer for different operations, avoiding lag and guaranteeing efficient functioning. RAM improves the system's multitasking skills by enabling the simultaneous operation of numerous programs. Lastly, data caching uses RAM to minimize the need to retrieve it from slower storage media, improving system efficiency overall, particularly for repetitive activities.

# SECTION 7: KM-01-KT07 : BIOS and CMOS 5%

**Understanding of BIOS and CMOS operations is demonstrated**

Together, the Basic Input/Output System (BIOS) and the Complementary Metal-Oxide-Semiconductor (CMOS) are two essential parts that set up and control a computer's basic functions during boot up.

**BIOS (Basic Input/Output System)**

BIOS is a firmware interface that initializes hardware components of a computer when it is powered on. It performs checks and setups to ensure all components are functioning correctly. The BIOS performs the Power-On Self-Test (POST) to check essential hardware components for errors before the operating system is loaded. If critical errors are detected, the BIOS alerts the user. The BIOS then executes the bootloader, a small program that loads the operating system into memory and hands control over to it. The BIOS determines the boot sequence and allows users to configure system settings related to hardware. It also manages low-level system functions, such as power management, thermal control, and hardware monitoring. Modern alternatives to BIOS include the Unified Extensible Firmware Interface (UEFI), which offers a more user-friendly interface, faster boot times, and support for larger storage devices. UEFI can coexist with BIOS in some systems, providing backward compatibility.

**CMOS (Complementary Metal-Oxide-Semiconductor)**

The BIOS settings of the computer, including the time and date, boot order, hardware configurations, and system passwords, are stored in the CMOS memory chip. The CMOS battery, a tiny battery located on the motherboard, powers it and keeps the settings intact even when the computer is turned off. A real-time clock (RTC) built into the CMOS chip records the current date and time as well as the system time. Through the BIOS/UEFI setup utility, users can change the CMOS settings, which include configuring system security features, boot priorities, and hardware component enable/disable.

In order to save configuration changes, load configuration data, and reset the system to its initial settings, the BIOS and CMOS communicate with one another. These adjustments are maintained between reboots by the CMOS battery. The system will, however, revert to its default settings if the CMOS battery dies or is removed. This frequently results in the loss of system time and date settings, requiring reconfiguration upon the next boot. A motherboard's standard problems and maintenance include updating the BIOS and clearing the CMOS, which returns the BIOS settings to their initial state. You can use a specialised jumper or remove the battery to clear the CMOS. In order to update the BIOS, the chip must be flashed with new firmware, which must be done carefully to prevent bricking the motherboard.

# SECTION 8: KM-01-KT08 : Hard drives and storage devices 5%

**An understanding of hard drives and storage devices and components is demonstrated**

A computer storage device is a hardware component that facilitates the storage of data and programs. Learn how to use them and obtain sample questions.

Storage Devices

Hard Disk Drives (HDDs) are computer systems that use magnetic storage to store and retrieve digital information. They consist of circular disks coated with magnetic material, a spindle that rotates the platters at high speeds, read/write heads that move across the platters for data reading and writing, an actuator arm that moves the read/write heads to the correct position, and a controller that manages data flow between the hard drive and the computer.

Solid-State Drives (SSD)s use flash storage, storing data as electric charges in cells, making them faster and more reliable than HDDs. They consist of NAND Flash Memory, a controller for data storage, retrieval, error correction, and wear leveling, and a DRAM cache for temporary data storage to speed up access times.

Hybrid Drives (SSHDs) SSHDs are hybrid drives that combine a traditional HDD with a small amount of SSD storage, improving performance and maintaining higher storage capacity. They consist of components similar to HDDs, with an added SSD portion for caching frequently accessed data.

Optical drives use lasers to read and write data on optical discs like CDs, DVDs, and Blu-rays. They consist of a laser diode, lens, spindle motor, and tracking mechanism. The laser emits the data, the lens focuses it on the disc surface, and the spindle motor rotates the disc.

USB flash drives are small, portable storage devices using NAND flash memory. They consist of a USB connector, NAND flash memory, and a controller that manages data transfer between the flash memory and the computer.

External hard drives are portable storage devices, typically HDDs or SSDs enclosed in a case with a USB interface for computer connection. They consist of an enclosure, an interface like USB, Thunderbolt, or eSATA, and a power supply, which can be external or through data connection.

# SECTION 9: KM-01-KT09 : Power supplies and voltage 5%

**Power supply and the effect on system hardware and components are explained**

**Power Supply Unit (PSU)**

The computer system's power supply unit (PSU), responsible for providing all other components with the electrical power they require, in order to function. Power is distributed to the motherboard, CPU, GPU, storage devices, and other peripherals through a variety of connectors and cables, and it transforms AC (Alternative current) to DC (Direct Current) and controls output voltage. Key components of a PSU include a transformer, rectifier, filter, regulator, and protection circuits.

Efficiency and power ratings are crucial when selecting a PSU. The total power that the PSU can offer is indicated by its wattage rating, which usually ranges from 300W to 1000W or more for high-performance systems. Higher efficiency ratings translate into lower electricity costs and less heat stress on components. Efficiency ratings (80 PLUS Certification) show how well a PSU converts AC power to DC power.

The motherboard has 24-Pin ATX connectors; the CPU has 4/8-Pin EPS connectors; the GPU has 6/8-Pin PCIe connectors; storage devices have SATA connectors; and some case fans and older peripherals have metal connectors. Selecting a PSU with sufficient wattage to sustain all system components—including those that may be added later—is essential.

# SECTION 10: KM-01-KT10 : Ports, cables, and connectors 2%

**An understanding of ports, cables, and connectors and the effect of voltage are demonstrated**

**Ports, Cables, and Connectors**

**Typical Connectors and Ports:**

* USB: Used to link devices such as portable storage units, printers, mice, and keyboards. USB-A, USB-B, USB-C, Mini-USB, and Micro-USB are among the types. Veloces differ.
* Ethernet (RJ45): Provides local and internet communication between computers and networks. Typical throughputs are 10/100/1000 Mbps.
* HDMI: Allows devices to exchange high-definition audio and video signals. There are two versions: HDMI 1.x and HDMI 2.x.
* DisplayPort: Used for high-definition audio and video signals, it is comparable to HDMI. DisplayPort 1.x and DisplayPort 2.0 are among the versions.
* 3.5mm audio jacks: These link external speakers, microphones, and headphones to the computer's audio system. Stereo audio and microphone input are examples of types.
* Thunderbolt: combines audio/video output with fast data transfer into a single port. Thunderbolt 3 and Thunderbolt 4 are among the speeds.
* VGA: Projectors and monitors utilise this outdated analogue video connector.
* Monitors use the DVI (digital video interface) connector. There are three types: DVI-I, DVI-D, and DVI-A.
* PS/2: Used to connect mouse and keyboard.

**Regulation of Computer System Voltage**

* Voltage Compatibility: Different components and devices need different voltage levels to function properly.
* Power Delivery: For gadgets like laptops and monitors, power adapters convert AC to DC.
* Overvoltage and Undervoltage: Overvoltage can cause sensitive components to be damaged by providing more voltage than is necessary.
* Voltage Regulation: The PSU controls and supplies steady voltages to each and every system component.
* Voltage regulators make sure that delicate parts like CPUs and RAM receive a steady voltage supply.

# SECTION 11: KM-01-KT11 : Networking and network operating systems 5%

**An Understanding of Wi-Fi USB Dongles**

Computers and other devices without integrated Wi-Fi can connect wirelessly thanks to USB dongles that support Wi-Fi. Since they are plug-and-play devices, no additional drivers are needed to connect them to a USB port. Usually, the operating system installs drivers automatically or includes them on a compact installation disc. Wi-Fi USB dongles support multiple Wi-Fi standards and work with a variety of operating systems, including Windows, macOS, and Linux.

The dongle usually has a normal USB connector that plugs straight into the USB port of a computer (USB-A or occasionally USB-C). A flexible or adjustable connector could be present in certain models to improve location and reception. For better signal reception, they could have an external or inbuilt antenna. LED indicators display signal strength, network activity, and connectivity status.

Standard Wi-Fi adapters, high-gain Wi-Fi adapters, dual-band Wi-Fi adapters, and Wi-MIMO and beamforming technologies are among the different varieties of Wi-Fi USB dongles. Standard Wi-Fi adapters are compatible with standard Wi-Fi standards; high-gain adapters can receive signals more clearly. Dual-band adapters offer flexible network connectivity by supporting both the 5 GHz and 2.4 GHz frequency bands.

# SECTION 12: KM-01-KT12 : Networking and wireless connections 3%

**Networking and wireless connections are discussed with reference to types and functionality**

In order to allow devices to communicate and share resources, networking and wireless connectivity are essential. Networks come in a variety of forms, each with unique features and applications. A local area network, or LAN, uses routers, switches, access points, PCs, printers, and other devices to connect devices within a certain geographic region, such as homes, workplaces, or campuses. With the use of routers, modems, leased lines, and network service providers, a wide area network (WAN) links devices over vast geographic areas, such as cities, nations, or continents. A metropolitan area network (MAN) uses network hubs, routers, switches, and fibre optics to connect devices throughout a city or big campus. Personal Area Network (PAN) connects devices within a very close range, such as a single room or a few meters, using Bluetooth devices, infrared devices, and storage devices.

Wireless connections provide flexibility and mobility by allowing devices to communicate without the need for physical cords. Wireless connections come in a variety of forms, each with unique features and applications. While Bluetooth allows for short-range wireless communication between devices, Wireless Fidelity (Wi-Fi) offers high-speed wireless connectivity for devices within a local area. Using 3G, 4G LTE, and 5G technologies, cellular networks provide wide-area wireless communication over mobile networks. Infrared (IR), which is frequently seen in remote controls and other outdated equipment, enables short-range communication via infrared light. Very short-range communication is made possible via near field communication (NFC), which is frequently utilised for data transfer between devices and contactless payments. Low-power wireless communication is offered by Z-Wave and Zigbee for Internet of Things and home automation devices.

One feature of networking is IP addressing, which gives each device on a network a unique address so that other devices can recognise and interact with them. Network protocols, such as TCP/IP, HTTP, and FTP, specify the guidelines for data transfer between devices. Network security uses firewalls, encryption, VPNs, and authentication protocols to guard data and resources against attacks and unauthorised access. Routing and switching transfer data packets between devices and networks.

# SECTION 13: KM-01-KT13 : Input and output devices 3%

**Input and output devices are identified and the respective functions are explained**

**Input Devices:**

* Keyboards are input devices that allow for text and command input.
* Mouse: Facilitates interaction with a graphical user interface.
* Scanner: Creates digital versions of hard copy documents.
* Microphone: Records or transmits audio for use in communication.
* Webcam: Recording or making video calls using captured video input.
* Touchscreen: Enables direct communication with the screen.

**Output Devices:**

* Monitor: Shows the computer's visual output.
* Printer: Generates hard copies of digital files.
* Speakers: Produce signals for audio.
* Headphones: Offers individualized audio output.
* Projector: Provides visual output for sharing media or presentations.

# SECTION 14: KM-01-KT14 : Installing and managing printers 2%

**An understanding of types of printers, installing printers and dealing with problems is demonstrated**

**Types of Printers and Installation**

• Inkjet printers: For colour documents and photos, use liquid ink.

• Laser Printers: Print text and graphics quickly and affordably by using a laser and toner.

• Dot matrix printers: For multi-part forms and harsh settings, use a print head.

Thermal printers, which are frequently used for labels and receipts, use heat to activate special paper.

**Setting Up Printers**

• Install drivers using the operating system, website, or CD provided by the manufacturer.

• Connecting: Use Bluetooth, Ethernet, or USB to connect a printer.

• Configuration: Use the control panel or software to set up printer preferences.

**Handling Issues**

• Troubleshooting: Make sure the printer has paper and ink/toner, inspect the connections, and switch it on.

• Driver Problems: Update or reinstall drivers if your printer isn't working properly or isn't recognised.

• Error Messages: Check online resources or the printer's manual.

• Print Quality: Crisp print heads or replace cartridges/toner if poor.

# SECTION 15: KM-01-KT15: Mobile devices, multimedia, and laptop computers 2%

**Troubleshooting procedures are explained**

**The process of troubleshooting is as follows:**

* Determine the Issue: Determine the precise problem and compile information.
* Reproduce: To comprehend the circumstances surrounding the issue, try to replicate it.
* Verify the basics: Make sure all hardware and cables are firmly attached.
* Consult Documentation: For guidance, consult user manuals or online documentation.
* Carry out simple fixes: In order to fix transient problems, restart the program or device.
* Isolate the Problem: Examine each piece of software or hardware separately. In order to isolate conflicts, boot into safe mode.
* Run Diagnostics: If required, use third-party diagnostic software or the built-in tools.
* Look for Conflicts: Find driver problems and software conflicts.
* Consult Support: For help, look through internet forums or get in touch with customer or technical support.
* Record and Test: Keep track of all modifications and troubleshooting procedures.

# SECTION 16: KM-01-KT16 : Preventative maintenance 2%

**The importance of preventative maintenance is justified**

Preventative maintenance is crucial for the health and efficiency of systems and equipment. It reduces downtime by identifying and fixing potential issues before they lead to significant failures, ensuring systems remain operational and reliable. Regular maintenance extends the lifespan of hardware and software by preventing wear and tear, keeping components functioning properly, and delaying the need for costly replacements. It also improves system performance by removing clutter, updating software, and adjusting settings, ensuring smooth and efficient operations.

Preventative maintenance also enhances security by updating software and applying security patches, protecting against vulnerabilities and reducing the risk of security breaches. It also leads to cost savings by addressing minor issues before they become major problems, ensuring compliance with industry standards and regulatory requirements, increasing reliability and predictability, and optimizing resource use. In summary, preventative maintenance is essential for maintaining system reliability, performance, and security while reducing costs and extending equipment lifespan. It proactively addresses potential issues, ensuring smoother and more efficient operations.

# SECTION 17: KM-01-KT17 : Troubleshooting procedures 2%

**Learning Outcome**

**Troubleshooting procedures are explained**

In order to determine the cause of the issue, the first step is to identify the problem, recognise its symptoms, and replicate them. Next, it examines power, error codes, and fundamental connections. It then looks to documentation for guidance, including user manuals or online documentation. After that, it carries out standard fixes like restarting the program or system and installing any available updates for drivers or software. After testing various parts or programs, it isolates the problem and boots into safe mode to find any conflicts or problems with drivers or software. After that, it performs diagnostics using internal or external tools as needed.

After that, it verifies that device drivers are compatible and up to date and looks for conflicts in the installed software or updates. If the issue continues or is beyond one's area of expertise, it then looks for assistance from forums or technical support. Lastly, it logs all of the modifications and troubleshooting steps, and tests the system to make sure the problem has been fixed. This method aids in tackling and resolving problems successfully.

# SECTION 18: KM-01-KT18 : Operating systems 5%

**Learning Outcome**

**Describe the big three operating systems: Windows, Linux, and Mac**

* Windows: Microsoft created this operating system, which is renowned for its intuitive user interface, broad software compatibility, and integrated security features. It is the industry leader in personal computer sales and finds application in corporate settings, video games, and consumer electronics.
* Linux: This open-source, highly configurable operating system was created by Linus Torvalds and is renowned for its robust security and stability. Package managers are used for updates and installation.
* MacOS: Designed by Apple Inc., it has a smooth, user-friendly interface, easy connectivity with Apple products and services, and strong security measures. It is most commonly used on Apple computers and is preferred by users who enjoy Apple's ecosystem as well as professionals in creative fields.

# SECTION 19: KM-01-KT19 : Managing files 2%

**Learning Outcome**

**Types of files and the respective purposes are identified**

**\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

# SECTION 20: KM-01-KT20 : Applications utility, troubleshooting, and optimization 2%

**Learning Outcome**

**Describe the Optimisation**

The process of optimising software and hardware systems improves their overall efficacy, performance, and efficiency. It includes a number of techniques to increase an application's or system's responsiveness and speed. These include application-specific optimisation, user experience optimisation, energy efficiency optimisation, network optimisation, security optimisation, resource management, database optimisation, network optimisation, system resource optimisation, and troubleshooting integration.

Performance optimisation is the process of reworking code, modifying resource usage, optimising database queries, indexing, and schema design, as well as optimising network optimisation, with the goal of making applications and systems run faster and more responsive. Utilising system resources like CPU, memory, and disc management as efficiently as possible is the goal of system resource optimisation. Application-specific optimisation, which includes configuration tuning, update management, and customisation, adjusts optimisations to the unique needs and behaviours of individual applications.

The goal of user experience optimisation is to enhance the overall user experience by increasing the responsiveness and intuitiveness of applications. Interface design, testing and feedback, load times, energy efficiency optimisation, bandwidth management, error correction, latency reduction, and security optimisation are some of the strategies.

Through bandwidth management, latency reduction, error handling, resource usage, update and patch management, and access control mechanisms, network optimisation seeks to increase the effectiveness and speed of network communications. In order to effectively address and resolve performance issues, troubleshooting integration combines optimisation efforts with troubleshooting. Continuous improvement, root cause analysis, and diagnostic tools are some strategies.

# SECTION 21: KM-01-KT21 : Configuring device drivers 5%

**Learning Outcome**

**Explain the considerations for configuring device drivers are reasoned**

Configuring device drivers is an essential step in making sure hardware works properly and effectively. Compatibility with the operating system (OS) and particular hardware, driver version and source, installation procedure, driver updates, driver conflicts, security, performance impact, backup and restore, documentation and support, compliance and legal considerations, and user impact are just a few of the important factors that need to be taken into account.

In order to avoid hardware issues, system instability, or even the OS not booting up, compatibility is crucial. Make sure the driver is compatible with the particular model and version of the hardware device and supports the operating system. Use the built-in OS update tools or get drivers from reputable sources, such as the official website of the hardware manufacturer or reputable retailers.

Versions of drivers can affect other software compatibility, performance, and stability. For optimal performance and bug fixes, stick with the most recent stable release; consider beta drivers only when necessary for additional features or enhancements. For the driver to function properly and integrate with the hardware and operating system, it must be installed correctly. If available, use automatic installation tools or adhere to the manufacturer's instructions.

Frequent updates can address security flaws, improve performance, and resolve bugs. Keep an eye out for problems like crashes or device malfunctions that might be related to driver conflicts, and utilise system tools to handle and resolve them.

Security is yet another crucial factor. If drivers are downloaded from unreliable sources, they may contain malware or other security risks. Use digital signatures to confirm the legitimacy of drivers, and scan them for malware prior to installation. Make sure drivers come from reliable sources to reduce security threats.

Impact on performance is yet another important driver configuration factor. In order to detect any adverse effects from driver updates, test new drivers for stability and performance impacts. You should also keep an eye on system performance and resource usage.

In the event that a new driver causes problems, backup and restore plans guarantee that users can return to a previous stable state. Before installing new drivers, make a backup of your current drivers and system settings. You can also use rollback functions or system restore points to return to a previous version of your software if needed.

Lastly, to avoid legal problems and guarantee appropriate software use, abide by licensing agreements and regulations. To handle driver updates or installations, make sure the user has the necessary permissions and training. By taking these things into account, you can make sure that device drivers are set up correctly, which will improve system security, performance, and stability.

# SECTION 22: KM-01-KT22 : Recovery 5%

**Learning Outcome**

**Describe what is a recovery partition?**

A recovery partition is a portion of an SSD or hard drive dedicated to storing files and tools for system recovery. In the event of a system failure, corruption, or other problems, it is intended to assist users in returning their computer to its initial configuration or reinstalling the operating system. System restoration, which returns the operating system to its original settings or a stable state without the need for external recovery media, and operating system reinstallation, which enables users to reinstall the operating system without the need for an additional installation disc or USB drive, as well as troubleshooting and diagnostics, which include tools for identifying and resolving system issues, are the two functions of the partition.

# SECTION 23: KM-01-KT23 : Cloud computing 5%

**Learning Outcome**

**Cloud computing functionality, benefits and risks are identified and described**

**Cloud computing functionality**

* Offers a range of service models, such as Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), and Public Cloud. • Provides scalable and on-demand resources.
* Provides programmatic access and integration via web-based access and API integration.

**Cloud computing benefits include:**

* Cost efficiency; pay-as-you-go; lower maintenance costs; global reach; scalable and flexible resources; disaster recovery and backup; remote access; security and compliance; innovation and agility.
* Risks include: provider lock-in, restricted control, limited customisation options, regulatory compliance, data sovereignty, downtime and service reliability, data security and privacy, and cost management.

**Risks of Cloud Computing**

* Cloud computing data security and privacy risks include possible breaches, privacy issues, dependencies on providers, downtime and service dependability, regulatory compliance, data sovereignty, cost management, vendor lock-in, loss of control, and customisation restrictions.

# SECTION 24: KM-01-KT24 : Security fundamentals 5%

**Learning Outcome**

**Typical security risks are listed**

**Common Security Risks to Computers**

**Malware**

* + Malware attaches to legitimate programs or files and spreads to other systems.
  + Viruses corrupt or destroy data, steal information, or disrupt system operations.
  + Worms: Self-replicating malware that spreads independently across networks.
  + Trojans: Malicious software disguised as legitimate software or files.
  + Ransomware: Encrypts files or locks users out of their systems until a ransom is paid.
  + Spyware: Secretly monitors and collects user information without consent.
  + Adware: Automatically displays or downloads unwanted ads.

**Phishing and Social Engineering**

* + Phishing: Fraudulent attempts to obtain sensitive information by pretending to be a trustworthy entity.
  + Spear Phishing: Targeted phishing attacks aimed at specific individuals or organizations.
  + Pretexting: Creating a fabricated scenario to obtain confidential information from individuals.
  + Baiting: Using a false promise or lure to trick individuals into downloading malicious software or revealing sensitive information.

**Unauthorized Access**

* Brute Force Attacks: Automated attempts to guess passwords or encryption keys.
* Credential Stuffing: Using stolen username-password pairs from one breach to gain access to accounts on other services.
* Privilege Escalation: Exploiting vulnerabilities to gain higher levels of access than initially granted.

**Network Attacks**

* + Man-in-the-Middle (MitM) Attacks: Intercepting and potentially altering communications between two parties without their knowledge.
  + Denial of Service (DoS) Attacks: Overloading a system, network, or service with traffic to make it unavailable.

**Exploits and Vulnerabilities**

* + Zero-Day Exploits: Attacks that target previously unknown vulnerabilities for which no patches or fixes are available.
  + Software Vulnerabilities: Flaws or weaknesses in software that can be exploited by attackers.

**Insider Threats**

* + Malicious Insiders: Employees or trusted individuals who intentionally misuse their access to cause harm.
  + Unintentional Insiders: Individuals who inadvertently cause security issues through negligence or lack of awareness.

# SECTION 25: KM-01-KT25 : Programming and development 5%

**Learning Outcome**

**Various software developments are listed**

**Software Development**

**Types of Software Development**

* Desktop Application Development: Creates software for desktop operating systems using C++, C#, Java, Electron,.NET, Qt.
* Mobile Application Development: Develops applications for mobile devices using platforms like iOS and Android.
* Web Application Development: Builds applications that run in web browsers using HTML, CSS, JavaScript, React, Angular, Vue.js, Node.js, Ruby on Rails.

**System Software Development**

* Operating Systems: Creates system software that manages hardware resources and provides services for applications.
* Firmware: Develops software that provides low-level control for hardware devices.

**Game Development**

* Video Game Development: Design and develop interactive games for consoles, PCs, and mobile devices.
* Simulation and VR/AR: Creates simulations and immersive experiences for training, entertainment, or research.

**Embedded Systems Development**

* IoT (Internet of Things): Develops software for interconnected devices that collect and exchange data.
* Embedded Systems: Design software for dedicated hardware systems with specific functions.

**Database Development**

* Database Design and Management: Creates and manages databases for storing and retrieving data efficiently.
* Database Administration: Maintains, optimizes, and secures databases.

**DevOps and Infrastructure Development**

* Continuous Integration/Continuous Deployment (CI/CD): Automates the process of integrating code changes and deploying software.
* Infrastructure as Code (IaC): Manages and provision computing infrastructure through code.

**Security Software Development**

* Cybersecurity Solutions: Develops software to protect systems and data from security threats.
* Secure Coding Practices: Implements coding practices that minimize vulnerabilities and enhance software security.

**Artificial Intelligence and Machine Learning**

* Machine Learning: Develops algorithms and models that enable systems to learn from data and make predictions.
* Natural Language Processing (NLP): Enables computers to understand and process human language.

**Software Development Methodologies**

* Agile Development: Promotes iterative development and collaboration to deliver software quickly and adapt to changes.
* Waterfall Development: Follows a sequential, linear process for software development.
* DevSecOps: Integrates security practices into the DevOps process to enhance security and compliance.