Hardware and Networking Service

Level-II

Based on March 2022, Curriculum Version 1



Module Title: - Implementing Maintenance Procedure

Module code: EIS HNS2 M08 0322

Nominal duration: 40 Hour

Prepared by: Ministry of Labour and Skill

April, 2022

Addis Ababa, Ethiopia

Table of Content

Acknoledgment
Introduction to the Module 5

Unit one: Equipment and software maintenance 6
1.1. Identification of equipment and software 7
1.2. Vendor documentation, peer organizations or research information 20
1.3. User Requirement 23
1.4. Documentation of maintenance procedure 26
Self-Check 1 29

Unit Two: Revision of appropriate practices 31
2.1. Maintenance operation 32
2.2. Service-Level Agreements 33
2.3. Change Assessment 34
2.4. Design and implementation of improved maintenance procedure 36
Self-Check 2 42

Unit Three: IT system components maintenance 43
3.1. Identification of warranty status 44
3.2. System architecture and configuration 45
3.3. Critical components and document recommendations 48
Self-Check 3 50

Unit Four: Maintenance procedures 51
4.1. Preventative maintenance 52
4.2. Maintenance procedure 57
4.3. Documentation and Approval of Recommended Procedure 60
4.4. Staff orientation about maintenance 62
4.5. OHS 63
Self-Check 4 67

Acknowledgment

Ministry of Labor and Skills and Ministry of Health wish to extend thanks and appreciation to the many representatives of TVET instructors and respective industry experts who donated their time and expertise to the development of this Teaching, Training and Learning Materials (TTLM).

Acronym

Introduction to the Module

This unit defines the competence required to set up maintenance procedures to keep equipment and software operating effectively and efficiently.

This module is designed to meet the industry requirement under the irrigation and drainage occupational standard, particularly for the unit of competency: **Implementing Maintenance Procedure**

This module covers the units:

- Equipment and software maintenance
- Revision of appropriate practices
- Identification of maintainable IT components
- Maintenance procedures

Learning Objective of the Module

- Determine best practices for equipment and software maintenance
- Revise practices, where appropriate
- Identify and analyze IT system components to be maintained
- Apply maintenance procedures

Module Instruction

For effective use this modules trainees are expected to follow the following module instruction:

1. Read the information written in each unit
2. Accomplish the Self-checks at the end of each unit
3. Perform Operation Sheets which were provided at the end of units
4. Do the “LAP test” giver at the end of each unit and
5. Read the identified reference book for Examples and exercise

Unit one: Equipment and software maintenance

This unit is developed to provide you the necessary information regarding the following content coverage and topics:

- Identification of equipment and software
- Vendor documentation, peer organizations or research information
- User Requirements
- Documentation of maintenance procedure

This unit will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Identify equipment and software to be maintained and implemented processes
- Identify vendor documentation, peer organizations or research information
- Obtain user Requirements
- Document maintenance procedure

1.1. Identification of equipment and software

1.1.1. Identifying computer hard ware to be maintained

There are several ways to identify the normal operation of a personal computer. Most people use diagnostic software packages like PC Tools, Norton Utilities and/or Check It to test a computer. Those diagnostic packages provide user-friendly operations to perform testing of a computer.

However, you can initially make measurable observations using your senses, that is, the sights and sounds to identify the normal operation of the computer. The table below suggests where to look and what you might hear to get an indication of normal behavior of a PC.

Table 1.1: Reference points for indications of normal behavior of a PC

Device	**Sights**	**Sounds**
System unit	Floppy disk drive activity indicator (light) Front panel indicators such as: • Power on LED (light emitting diode) • Hard disk drive activity LED	Floppy disk drive mechanisms Speaker (beep) Fan Hard disk drive
Display unit (monitor)	Power on indicator Text displayed on screen	
Keyboard	**Num lock** indicator **Caps lock** indicator **Scroll lock** indicator	
Printer	Power on indicator	Tractor feed

	Online/ready indicator Busy indicator Message display indicator	Printer head Laser printer mechanisms
Mouse	When software is loaded, mouse pointer appears on a screen that reflects a correct positioning of a pointer, or other operations of a mouse	

Potential sources of damage to computer hardware and software

There are a number of common causes of damage to a computer or its components. These are:

- ✓ Temperature variations
- ✓ Power cycling
- ✓ Static electricity
- ✓ Power line noise
- ✓ Radio frequency interference
- ✓ Phosphor burn on a monitor
- ✓ Dust and pollutants
- ✓ Water

➢ **Temperature variations Cause**

Temperature variations (expansion and contraction of components from temperature change) can lead to serious problems.

Damages

- Chip creep: where the heating and cooling of components can cause

movement, usually out of the socket that holds the component.

- Signal traces on circuit boards can be cracked and separated.
- Solder joints can be broken.
- Contacts undergo accelerated corrosion.
- Solid-state components can be damaged.
- Read and write problems on hard disk drive (due to expansion and contraction of the platter of hard disk the data may be written at a different location relative to the track center).

Advice

- Ensure a computer operates in correct ambient temperature Refer to the computer User‘s Manual for this information.
- Ensure the ambient temperature when the:
- system is **on** it is in the range of **15-32 °C**
- System is **off** it is in the range of **10-40 °C**.

➢ **Power cycling**

Cause

Turning on a cold computer subjects it to the greatest possible internal temperature variation.

Damages

Same as for temperature variation

Advice

Power on a computer only once daily. Don‘t turn a computer on and off several times every day.

- **Static electricity**

Cause

This problem usually appears during winter months when humidity is low, or in extremely dry climates where the humidity is low year-round.

Some static-sensitivity problems are caused by improper grounding of computer power.

Damages

Electronic components

Advice

- Always use a three-prong, grounded power cord plugged into a properly grounded outlet. You could use an outlet tester to check that it is properly grounded, but today, OH&S requires that all power equipment be properly tested and certified. This includes the outlets, cables and connectors.
- Use a grounded static mat underneath a computer, or an antistatic wrist-strap, before touching internal components of the computer.

- **Power line noise**

Cause

This problem is caused by poor quality power being supplied to a computer system, which creates some spikes and transients (short transient signals of sometimes 1000 volts or more).

It can also be caused by sharing a power source with other higher power consuming equipment, such as coffee makers, copy machines or a laser printer.

The wire size and length will affect the resistance of a power circuit.

Damages

All system components

Advice

- A computer system should be on its own circuit with its own circuit breaker.
- A three-wire circuit is a necessity.
- To decrease resistance, avoid extension cords unless absolutely necessary and then use only heavy-duty extension cords.
- Avoid using too many items on a single outlet.
- Add an Uninterruptible Power Supply (UPS) as a power conditioner.

- **Radio frequency interference**

Cause

Mobile phones, cordless phones, fax machines and any radio transmission equipment

Effects

- Sporadic random keystrokes will appear, as though an invisible entity were typing on the keyboard
- White spots and lines appear on the screen

Advice

- Install specially shielded cables (built-in toroid core cables) outside a system unit.

- **Phosphor burn on a monitor**

Cause

The phosphor on a cathode ray tube can be burned if a stationary image is left on a screen continuously for long time.

Damages

Reduces the life of monitor (cathode ray tube)

Advice

- Turn both brightness and contrast levels to the minimum.
- Use a screensaver that displays different patterns on a screen.

- **Dust and pollutants Cause**

A power supply fan carries airborne particles through a computer.

Food crumbs are attracted by magnetic media, while cigarette ash and smoke are drawn toward disk drives.

Damages

- Floppy disk heads and media
- Electronic components (dust on the surface of components prevents necessary heat loss)

Advice

- Use power supply unit with air filter (the filter must be cleaned and changed periodically).
- Don‘t operate an unprotected computer in a dusty environment, eg an industrial workshop.

- **Water Cause**

On a desktop, coffee or tea spills over a keyboard or into a monitor.

Damages

- Keyboard malfunction
- Monitor explosion (if a monitor is on)

Advice

Never eat, drink or smoke inside a computer room.

1.1.2. The first steps towards troubleshooting Reflect

Here is a typical scenario reported to the help desk.

A client phones the help desk and reports that the computer hangs each time they try to run a particular application.

- What might be the source of the problem?
- What steps will you take to find out? This is the trouble shooter‘s challenge! ***Feedback***

In all cases where you are trying to troubleshoot a problem, you need to use a **logical step-by-step approach**. For example, two questions that you would always ask in this situation are:

- When did the problem begin?
- Has any new hardware or software been added between the times that the problem appeared and when the system was last working correctly?

Here is a list of reasons why a computer might hang each time a specific software application is run. It could indicate:

- a corrupted file
- an incorrect installation
- hard disk failure
- a virus
- a new application causing conflict
- new hardware causing conflict
- New device drivers causing a conflict with older software.

General troubleshooting guide

Here‘s a general troubleshooting guide that you can use when a computer develops a fault.

- ✓ Don‘t panic.
- ✓ Observe:
  - What are the symptoms?
  - What conditions existed at the time of failure?
  - What actions were in progress?
  - What program was running?
  - What was displayed on the screen?
  - Was there an error message?
  - What functions are still working?
- ✓ Use your senses (sight, hearing, smell and touch).
  - Is there any odor present?
  - Does any part of the system feel hot?
- ✓ Check power supply:
  - Is the plug inserted snugly into the computer?
  - Is the power cord plugged into an appropriate wall power outlet?
  - Is the wall power outlet working?
- ✓ Documentation (fill in a pre-designed check list):
  - What is the computer doing?
  - What is the computer not doing?
  - What is being displayed on the screen?
  - Is there any error message?
  - What is still operating with everything connected?
  - Is power still operating on each part of a computer?
- ✓ Assume one problem:
  - Use correct data and resources
  - Use relevant technical manuals and information
  - Use proper test equipment.
  - Isolate units one-by-one:

- If a system worked when all peripherals were disconnected, turn power off and reconnect one of the peripherals. Power on and test. If that unit works, turn the power off and reconnect another peripheral. Again, power up and test. Follow this procedure until a unit fails.

✓ Consult your index of symptoms:

- Using your logbook, help desk database, or any relevant flow charts in reference books and manuals.

✓ Localize to a stage.

✓ Isolate to the failed part.

✓ Test and verify proper operation.

After diagnosing and rectifying the fault, you need to document it in the log book or help desk database for future reference.

1.1.3. A hardware fault-finding checklist

Here‘s a useful checklist that you can use to help you diagnose faults in hardware.

- First, consult any service level agreements (SLA) to ascertain if or clarify response time obligations and internal/external responsibilities. Determine also if there are there any other organizational guidelines you need to follow.
- Consult documentation logged from previous related or similar situations. Determine a set of questions can you ask the user, your colleagues and your supervisor that might assist you in finding a solution.
- Remember to keep safety as your highest priority by observing OH&S precautions, that is, ensure your own safety first, and then consider other precautions such as static discharge, etc.
- Check the power supply. Ensure it is working and that it is powering the motherboard.
- If no video is displayed try swapping the monitor with a known good one.
- If the video controller is built in, disable it and try another known working video card. To disable the built in video controller you will need to access the system CMOS or BIOS

Setup. On some systems, simply inserting a new video card will automatically disable the built in video.

- Remove all expansion cards. If the machine boots, replace the cards one by one until the problem reappears.
- Check the CPU fan is operating.
- Check the RAM chips by swapping them with known good ones.
- Check the motherboard for signs of blown components.
- If still no success, you might swap the entire motherboard and CPU.

Remember to document everything you do according to organizational guidelines.

Is the problem with the hardware or the software?

A computer system consists of a hardware sub-system and a software sub-system. However, when looking for the cause of the fault, sometimes it can be difficult to determine if the fault is hardware or software. Once you have determined that the fault is confined to one of these two sub-systems, you can then isolate it, focus on the fault-finding process, and rectify the fault.

The easiest way to determine whether a problem is hardware or software is to test the hardware with software packages that are known to be good and that have successfully run on the system before. If the system boots and operates correctly, then the fault can be put down to software. If the system does not boot or operate correctly then the fault can be put down to hardware.

Configuration problems

Configuration problems are problems that arise when a computer system is set up for the first time or when new peripherals/components are added to the system. When the component is first added, the system is not ready to receive the hardware, until the system is prepared to support the device. This mismatch can be rectified by:

- installing the appropriate software device drivers
- configuring CMOS/BIOS
- Configuring the operating system.

The POST

The Power On Self-Test (POST) operates whenever a computer is switched on.

Whenever you start up the computer system, the computer automatically runs a series of tests. These test the basic functionality of vital components such as the CPU, RAM, video card, motherboard, and input and output devices.

POST tests are not particularly thorough, but they represent the first line of defense, especially in handling severe motherboard problems. If the POST test finds a problem which is severe enough to keep the system from operating properly, it halts boot up of the system and produces audio beeps and/or error messages. You can find the meanings of these error signs in documentation from the system manufacturer — this is often required for an accurate understanding of audio beeps and messages. But if the POST fails, then at least you know the problem is hardware-related.

The boot up process

Carefully watching the steps in the boot process can reveal a lot about the nature of problems in a system. By doing this you can include or exclude various possible causes of faults. The absence of one or more of the following during booting can indicate a fault:

- ✓ When power is applied, the power supply fan should work.
- ✓ The keyboard lights should flash as the rest of the system components are reset.
- ✓ A POST memory count and test should be seen.
- ✓ A BIOS message should be visible on the monitor.
- ✓ The floppy drive access light should come on briefly.
- ✓ The hard disk access light should come on briefly.
- ✓ An audible short beep should be heard.
- ✓ The floppy disk access light should come briefly before a check of the hard drive starts.
- ✓ An operating system prompt, message, or logo should be visible.

By observing the above sequence you should be able to work out where the problem might be, that is, isolate the fault. For instance, if any of the above steps (except the last one) fails in some regard, then you know the problem is hardware-related.

Hardware toolkit

What equipment are you likely to need when carrying out the fault-finding? The most useful tool, which you should never leave home without, is a good quality Philips-head screwdriver. However, other tools in your hardware toolkit may include:

- screwdrivers — a full set and range of sizes
- anti-static strap
- pointy-nose pliers
- multi meter
- known good components such as video card, cables, mouse, hard-disk drive, network interface card (NIC), CD-ROM drive
- serial and parallel loop-back connectors
- boot disks
- a range of testing software for the loop-back plugs and NIC
- a POST card.

POST cards

A POST card is a device that plugs into an empty slot in the motherboard. When the system boots up, the card runs a series of diagnostics. In some cases these cards replace the normal functions of the BIOS. The great advantage of using these cards is that you do not have to resort to software running off the hard drive or a floppy disk.

POST cards are normally used when systems are _dead‘, or when the system cannot read from the hard drive or the floppy drive. Typically, a normal BIOS chip stops when there‘s a severe error condition. POST cards can actually continue and go through a full testing cycle. Some POST cards also come with a series of light emitting diodes (LEDs) that produce coded error signals that you could interpret together with a manual. Other cards produce audio beep signals.

Diagnostic software

There is a wide range of diagnostic tools available that can help you identify all sorts of computer problems. Generally, the diagnostic software used for testing system components and/or performance falls into two categories:

- Generic
- Proprietary

Generic diagnostic software

The generic tools available are usually sold as software packages and are very limited. To evaluate the usefulness of generic software you have to assume that the software supplier has tested their software with all original equipment manufacturer (OEM) hardware and software you may want to test. This is hardly possible, so you should not be surprised when the results of such packages fail to live up to expectations.

This is not to say the providers of these packages are supplying a defective product — just that they can really only test the functionality of devices and systems functions known to the program writers and this will exclude many proprietary devices. A good example of this would be network interface cards (NICs).

Most of the generic diagnostic packages will probably be able to determine that the NIC is installed in the system, however, if the exact functionality instructions of the NIC are not built into the diagnostic software, an accurate result will probably not be achieved.

This is better understood when considering that the same NIC OEM may provide a different diagnostics utility with each of many similar NICs. If the wrong version of the diagnostics utility is tried with the wrong NIC, even the most basic loop-back test will often fail. This highlights the need to pay close attention to the software provided by OEMs.

Another factor to consider is that general diagnostic software uses information gained from the underlying operating system, which gains its information from the BIOS. This means that the operating system (using its device driver) may not be able to accurately provide information on the device.

If the information provided to the diagnostic software is not extremely accurate, then valid test results are not a reasonable expectation.

For truly accurate testing of a device you should use the software provided by the manufacturer or use specialized diagnostic software that can bypass the operating system all together.

1.1.4. Software tools

Propriety diagnostic software

If diagnostic software is operated on its own specially designed operating system, then direct access (via the BIOS) to the hardware will likely yield accurate and thorough details. Having unimpeded access to the low-level functions of the hardware means the diagnostic software is able to run rigorous testing and reporting. After all, it‘s unlikely that rigorous memory testing could be performed while there are several other programs currently running in memory.

Two examples of good diagnostic software are:

- Micro-Scope Diagnostic Suite from Micro2000 (http://www.micro2000.com/)
- PC Certify Lite from Pro Tech Diagnostics (http://www.protechdiagnostics.com/)

Common diagnostic tools

All operating systems come with utilities that are used for general checking, repair and reporting of faults. Each operating system is different but they do have some tools in common such as hard disk scanning tools, eg:

- Scandisk for Microsoft
- fsck (file system check) for Unix clones like Linux
- Disk First Aid for Apple MacIntosh systems.

If your operating system supports it, then checking the device interrupts and input/output addresses can locate problems associated with hardware conflicts, or apparent inoperative hardware. For instance, you may have a sound card installed in a system but have difficulty in getting the device to produce any sound, when you know the device is not faulty. You would know the device operates correctly if you install it in another computer and can play audio.

When using any of the diagnostic tools, especially the disk checking utilities, the operator and other system users must be considered. As hard drives have become larger in size, the time taken to check them has also increased, to the point where it can take hours to fully complete some of the diagnostics. These checks do need to be carried out regularly but should be programmed to be done at a time outside usual working hours or by arrangement with the clients/users.

Leave a trail to follow

Apart from the use of diagnostic software (and a little trial and error) examining documentation on past faults and their solutions can reveal a lot. To give two examples:

- The introduction of a new device (say a different brand of NIC) may bring with it some configuration problems. If there is documented evidence of previous problems, together with information on how the problem was solved, you can more efficiently remedy similar problems. The remedy may come in the form of an automated configuration file (script), or a decision to purchase less trouble-prone devices.
- The reports generated by some help desk software may indicate that a particular user consistently experiences problems with certain devices, or software applications. This

information could then be used to reduce future incidents of support calls by providing or recommending targeted training for that user. The term currently in use for this is ’just in time training‘(JIT).

For this approach to work, you must leave a documented trail to follow. The main consideration is to record and/or document all problems, changes made, and when they happened. The job is not finished until the documentation is done. Documentation needs to be done in accordance with standard organizational guidelines.

Finding more information

Experience, a logical approach and reviewing previously documented problems and solutions, can form the backbone of being able to analyze and determine the cause of system faults. However, there is always something new and no single person or group can form the only valid source of good information. There will always be a need to perform some research as a result of some fault or problem caused by hardware or software. The Internet provides other sources of information that can be relied upon.

When you do research on the Internet, you should check the source of the information, and bookmark (add to favorites) those that you consider valid and useful.

In the **Research** section of this Learning Pack you‘ll find many websites to carry out further research of the topics discussed here, including hardware-related and software-related websites.

1.2. Vendor documentation, peer organizations or research information

Manufacturers should be able to demonstrate that they have a commitment to environmental good practice, and that their equipment has been designed with environmental impacts in mind. Most ICT equipment available in the world is manufactured overseas, so there is limited opportunity to influence the design of the equipment.

However, maintaining ICT equipment should require suppliers to provide information on the steps being taken by the manufacturer to reduce the environmental impact of their products. In some regions of the world, such as Europe and North America, governments are increasingly regulating the manufacturing process to reduce waste.

Manufacturers are also starting to adopt Corporate Social Responsibility (CSR), which recognizes an obligation to consider the interests of customers, employees, shareholders, communities, and ecological considerations in all aspects of their operations. This obligation is seen to extend beyond their statutory obligation to comply with legislation.

The Eco-Management and Audit Scheme (EMAS) is the EU voluntary instrument which acknowledges organizations that improve their environmental performance on a continuous basis. EMAS registered organizations are legally compliant, run an environment management system and report on their environmental performance through the publication of an independently verified environmental statement. They are recognized by the EMAS logo, which guarantees the reliability of the information provided.

Fewer toxic components In January 2003 the European Parliament and the Council of the European Union issued a RoHS (Restriction of Hazardous Substances) Directive 2002/95/EC on the restriction of the use of certain hazardous substances in electrical and electronic equipment, and Directive 2002/96/EC on waste electrical and electronic equipment.

The two directives were designed to tackle the fast-increasing waste stream of electrical and electronic equipment. Directive 2002/96/EC requires increased recycling of electrical and electronic equipment to limit the total quantity of waste going to final disposal.

It also requires producers to take responsibility for taking back and recycling electrical and electronic equipment. This is intended to provide incentives for manufacturers to design electrical and electronic equipment in an environmentally more efficient way, which takes waste management aspects fully into account. Consumers should be able to return their equipment free of charge.

In order to prevent the generation of hazardous waste, Directive 2002/95/EC requires the substitution of various heavy metals (lead, mercury, cadmium and hexavalent chromium) and brominated flame retardants (polybrominated biphenyls [PBB] or polybrominated diphenyl ethers [PBDE]) in new electrical and electronic equipment put on the market from 1 July 2006.

The directive does, however, provide for some exemptions, including lead in the glass of CRTs and mercury in lamps for flat-panel displays. Although RoHS compliance has not been legislated in New Zealand, many other countries are following the European Union‘s lead, some with their own variations (as in China), and it is widely expected that RoHS will become a world-wide standard. There is no recognized logo for RoHS but manufacturers have chosen their own way to display compliance with the EU RoHS Directive.

❖ **Using recycled content**

In 1999 a computer supplier announced the world‘s first desktop PC using 100 per cent recycled plastic in all the plastic parts. However, it appears this was not commercially sustainable, and the company‘s 2006 Corporate Responsibility Report states that 28 per cent (by weight) of all plastic resins contain recycled plastic content, with a net recycled plastic content weight representing 8.1 per cent of total purchases (against a corporate goal of 5 percent).10 The EU RoHS Directive precludes the use of some recycled materials because of the use of substances such as flame-retardant bromides.

❖ **Some Examples of hard wares include:**

- LCD display screens

Liquid crystal displays (LCDs) consume about half the power of an equivalent-sized cathode ray tube (CRT) screen. LCDs also have direct user benefits in terms of saving desk space, and they are better for your health.

CRT monitors radiate three electron beams that are continually refreshing the entire screen 60 to 85 times each second. Although your brain doesn‘t register the constant refreshing, your eyes do, and they have to work harder to absorb the information. LCD monitors don‘t refresh in this way: pixels are constantly on or off, which greatly reduces eye fatigue and strain. An LCD monitor also generates less heat than a CRT, lessening the air conditioning loads in an office.

- Desktop printers

Desktop printers, while convenient for users, can be costly to maintain and operate. On the other hand, when printers are networked and shared among groups of users (the most common scenario), no one is responsible for turning them off at night. Current good practice is to consolidate printing functions into networked MFDs that are deployed on the basis of one per floor.

As noted above, MFDs have good power management tools and duplex printing (both sides) can be set as a default. Desktop printers typically have less functionality than MFDs and only more recent models have started to provide duplex printing as a default option. The Ministry for the Environment provides sustainability guidelines for office consumables such as paper and ink cartridges.

1.2.1. Impact of ISO on ICT

In the 1980s ISO began the work of devising ―process‖ standards, specifically the ISO 9000 Quality Management System standards. Firms in the ICT industry want to become ISO certified in order to improve their business practices and retain business with certain customers. More than 90% of ICT companies worldwide work within the needs of standardization. The term standardization is used in ICT companies to measure the quality of their services.

Applying ISO in ICT companies is considered to be significant in that it allows these companies to implement the total quality management (TQM) strategy to improve their organizational performance (Magd, 2006).

ICT practices have used many ISO standards such as ISO 9001 QMS, ISO 20000 ITSM, ISO 27001 ISMS and other standards. For example, ISO 9001 QMS helps bring out the best in organizations by enabling people to understand the processes of delivering products/services to customers.

- **ISO's Quality Management System**

is a model for continual improvement and customer satisfaction, and any organization looking to improve how it functions or does business can use it, regardless of size or sector. ISO 20000 ITSM promotes the adoption of an integrated process approach for effectively delivered managed services to meet business and customer requirements. To take another example, ISO 27001 ISMS provides information to responsible parties for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management Systems (ISMS). It also designed to ensure adequate security controls that protect information assets, document ISMS and give confidence to customers and interested parties.

1.3. User Requirement

The User Requirement document is a specification of requirements from the user point of view, and its contents are thus essentially non-technical.

It is not mandatory for the specification to include any technical elements. However, the users often do have technical requirements, and when they do such requirements have to be included in the User Requirement document. But even then they must be presented so as to be capable of being understood by the non-technical reader. The users will usually rely upon the services of appropriate technical advisors to help in the specification of such requirements.

- Hardware requirements

If hardware is to be supplied, it warrants its own detailed requirements section. This should specify requirements in a little or as much detail as the users care about the matter. A minimal specification might be concerned just with the general nature, capacity and performance of the equipment to be provided. But the defined requirements might even, for reasons of compatibility or standardization, go so far as to specify particular makes and models of equipment, if that is what the user community wants.

1.3.1. Business requirements

Business requirements, also known as stakeholder requirements specifications (StRS), describe the characteristics of a proposed system from the viewpoint of the system's end user. Products, systems, software, and processes are ways of how to deliver, satisfy, or meet business requirements

Confusion arises for three main reasons.

- A common practice is to refer to objectives, or expected benefits, as 'business requirements.'
- People commonly use the term 'requirements' to describe the features of the product, system, software expected to be created.
- A widely held model claims that these two types of requirements differ only in their level of detail or abstraction — wherein 'business requirements' are high-level, frequently vague, and decompose into the detailed product, system, or software requirements.

Such confusion can be avoided by recognizing that business requirements are not objectives, but rather meet objectives (i.e., provide value) when satisfied. Business requirements what's do not decompose into product/system/software requirement how's. Rather, products and their requirements represent a response to business requirements — presumably, how to satisfy what. Business requirements exist within the business environment and must be discovered, whereas product requirements are human-defined (specified).

Business requirements are not limited to high-level existence, but need to be driven down to detail. Regardless of their level of detail, however, business requirements are always business deliverable what's that provide value when satisfied; driving them down to detail never turns business requirements into product requirements.

In system or software development projects, business requirements usually require authority from stakeholders. This typically leads to the creation or updating of a product, system, or software. The product/system/software requirements usually consist of both functional requirements and non-functional requirements. Although typically defined in conjunction with the product/system/software functionality (features and usage), non-functional requirements often actually reflect a form of business requirements which are sometimes considered constraints. These could include necessary performance, security, or safety aspects that apply at a business level.

Business requirements are often listed in a Business Requirements Document or BRD. The emphasis in a BRD is on process or activity of accurately accessing planning and development of the requirements, rather than on how to achieve it; this is usually delegated to a Systems Requirements Specification or Document (SRS or SRD), or other variation such as a Functional Specification Document. Confusion can arise between a BRD and a SRD when the distinction between business requirements and system requirements is disregarded. Consequently, many BRDs actually describe requirements of a product, system, or software.

- **Benefits of Business Requirements**

Table 1.2. Business Requirements

	Description
ReduceProject failure	Structured explanation of a business process or method defined early in the life cycle helps reduce project failures that occur due to misaligned or misrepresented requirements leading to failure of user expectations.
Connect Broader business goal	Well-defined business requirements help lay out a project charter, a critical to step in executing business strategy or business goals, and to take it to the next logical step of developing it into an IT system. This helps monitoring overall project health and provides for positive traction with key project stakeholders including sponsors.
Consensus creation and collaboration	The benefit of a structured format typical of business requirements documentation helps create positive consensus and better collaboration where the business stakeholder group

	might be a large cross-functional team, distributed geographically.
Saves costs	Good quality of business requirements when captured early on not only improves success of a project but also save overall costs associated with change requests, and related investments in training, infrastructure, etc.

❖ Difficulties of Business requirement

Business requirements are often prematurely hardened due to the large stakeholder base involved in defining the requirements, where there is a potential for conflict in interests. The process of managing and building consensus can be delicate and even political by nature. A lesser challenge, though common, is that of distributed teams with stakeholders in multiple geographical locations. It is natural that sales staff is closer to their customers, while production staff is closer to manufacturing units; finance and HR, including senior management are closer to the registered headquarters. A system for example that involves sales and production users may see conflict of purpose – one side may be interested in offering maximum features, while the other may focus on lowest cost of production. These sorts of situations often end in a consensus with maximum features for a reasonable, profitable cost of production and distribution.

1.4. Documentation of maintenance procedure

A maintenance procedure is only as good as its measurement data. Poor data may be worse than no data at all because poor data may lead to the wrong analysis, resulting in working on the wrong thing.

One of the best ways to help ensure good data collection is to have well-written procedures. Plants often fail to see the importance of having well-written procedures for most tasks and especially for tasks seemingly as simple as data collection.

Why are Standard Maintenance Procedures Necessary?

- To protect the health and safety of employees.
- To help ensure that everyone performs a task to the same degree of precision.
- To save time when performing a task.
- To help ensure that standards and regulations are met.
- To minimize the effects of personnel turnover.
- To increase equipment reliability.
- To serve as a training document.
- To help document the equipment management procedure.
- To help protect the environment.
- To provide a basis for accident investigation

What Information Should be contained in a Standard Maintenance Procedure?

- Formal title and document number.
- A statement reading: "Read all of the steps in this standard maintenance procedure before beginning work."
- Personal protective equipment (PPE) required to do the job.
- All safety and environmental hazards to be aware of while doing the job.
- A detailed list of steps for performing the job or task.
- A complete list of tools and materials for doing the job.
- References to other documents needed to perform the job.
- Photos and diagrams where needed to explain job steps.
- Measurements, standards and tolerances in the standard maintenance procedure steps.
- Any other important information that may help the worker complete the task in a satisfactory manner.
- A definition of skills required for performing the job.

- Hours required to perform the job.
- Number of people required to perform the job.
- Required frequency of performing the job.
- Preparation and revision dates.
- Approval and review signatures.
- Space to provide feedback as to the accuracy and effectiveness of the standard maintenance procedure.

Feedback is critical to the success of SMPs. In order for SMPs to be effective and accurate, a formal feedback mechanism should be supplied to the job performer. The SMP should be updated when feedback reveals mistakes or more effective ways to perform the job. Poorly written SMPs are unsafe and largely ineffective.

Who should write standard maintenance procedures?

- A person who has some training in writing SMPs and who knows his or her company's SMP writing procedure. (Yes, there should be a procedure for writing procedures.)
- A person knowledgeable about the safety and environmental hazards involved.
- The writer should seek input from the trained job performer or subject matter experts who will be using the SMPs. It is a good idea to get the job performer to write the rough draft because you will get buy-in from the SMP users. A person is much more likely to use something that they helped to develop as opposed to something that was developed without his or her input.

What are the rules for writing standard maintenance procedures?

- The burden of written communication is on the writer, not the reader. The goal is to serve the user.
- The first writing is a rough draft and will need to be reviewed and tried before being published.
- Use numbered line items and avoid paragraphs (one item per step).
- Keep wording short and precise.
- List steps in proper sequence. The job should flow in natural order.
- Use step check-offs where useful.
- Have the job performer enter quantitative values; it is even better than check-offs.
- Target elementary-grade reading level (fourth or fifth grade) if possible, given the nature of the procedure being written. A reading skill commensurate to the minimum qualifications for performing the job itself is assumed.
- Use graphics where needed to clarify meanings. A picture really is worth a thousand words.
- Keep verbiage consistent. Don't change equipment names from step to step.

- Begin each step with a verb if possible. For example: Step 13 - Remove coupling guard.
- If jobs involve too many steps, break the job into sections such as Motor Removal Section and Gear Unit Removal Section

Self-Check 1	Written Test

Name:_____ Date:_____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

A. Choose the correct answer from the given alternatives

1. Reasons why a computer might hang each time a specific software application is run

A. corrupted file C. hard disk failure

B. an incorrect installation D. All

2. During Power supply checking which question is correct?

A. Is the plug inserted snugly into the computer?

B. Is the power cord plugged into an appropriate wall power outlet?

C. Is the wall power outlet working?

D. All

3. Among the following which one is diagnostic tool?

A. Scandisk for Microsoft

B. fsck (file system check) for Unix clones like Linux

C. Disk First Aid for Apple MacIntosh systems

D. All

4. Which one is not hard ware toolkit?

A. Screwdrivers C. Anti-static strap

B. Anti-virus D. All

B. Write True if the statement is Correct and False if the statement is Incorrect

1. The Eco-Management and Audit Scheme (EMAS) is the EU voluntary instrument which acknowledges organizations that improve their environmental performance on a continuous basis.

2. Liquid crystal displays (LCDs) consume about half the power of an equivalent-sized cathode ray tube (CRT) screen.

3. CRT monitors radiate three electron beams that are continually refreshing the entire screen 60 to 85 times each second.

4. CRT monitor generates less heat than a LCD, lessening the air conditioning loads in an office.

C. Fill the blank

1. _____ is also known as stakeholder requirements specifications.
2. _____ Document is a specification of requirements from the user point of view, and its contents are thus essentially non-technical.
3. _____ Rule is used for writing standard maintenance procedures?

Unit Two: Revision of appropriate practices

This unit to provide you the necessary information regarding the following content coverage and topics:

- Maintenance operation
- Service-Level Agreements
- Change Assessment
- Design and implementation of Improved maintenance procedure

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Review and Monitor Maintenance operation
- Identify Problem areas to meet service-level agreements and considering changes
- Assess Changes in consultation with appropriate person
- Design and implement Improved maintenance procedure

2.1. Maintenance operation

The Monitoring Maintenance Lifecycle (MML) is a monitoring development process to reduce maintenance costs and increase reliability of IT infrastructure concerning service recovery related problems. It is based on the classical Waterfall model.

Monitoring Maintenance Lifecycle are methods and standards for improving and mastering maintenance processes, supporting processes and management processes throughout the monitoring lifecycle.

After the procedure is implemented to the organization its progress is measured and its benefit is compared with the previous maintenance mechanism used by that organization.

2.2. Service-Level Agreements

A service-level agreement (SLA) is a contract between a service provider and its internal or external customers that documents what services the provider will furnish and defines the service standards the provider is obligated to meet

➢ Why are SLAs important?

Service providers need SLAs to help them manage customer expectations and define the circumstances under which they are not liable for outages or performance issues. Customers can also benefit from SLAs in that they describe the performance characteristics of the service, which can be compared with other vendors' SLAs, and also set forth the means for redressing service issues -- via service credits, for example. For a service provider, the SLA is typically one of two foundational agreements it has with customers. Many service providers establish a master services agreement to establish the general terms and conditions in which they will work with customers. The SLA is often incorporated by reference into the service provider's master services agreement. Between the two service contracts, the SLA adds greater specificity regarding the services provided and the metrics that will be used to measure their performance.

➢ What goes into an SLA?

In broad terms, an SLA will typically include a statement of objectives, a list of the services to be covered by the agreement and will also define the responsibilities of the service provider and customer under the SLA.

The customer, for example, will be responsible for making a representative available to resolve issues with the service provider in connection with the SLA. The service provider will be responsible for meeting the level of service as defined by the SLA. The service provider's performance is judged according to a set of metrics. Response time and resolution time are among the key metrics included in an SLA, since they relate to how the service provider deals with a service interruption.

➢ Penalties: Repercussions for breaking terms

In addition to establishing performance metrics, an SLA may include a plan for addressing downtime and documentation for how the service provider will compensate customers in the event of a contract breach. Service credits are a typical remedy. Here, the service provider issues credits to the customer based on an SLA-specified calculation. Service providers, for

example, might provide credits commensurate with the amount of time it exceeded the SLA's performance guarantee.

A service provider may cap performance penalties at a maximum dollar amount to limit exposure.

The SLA will also include a section detailing exclusions, that is, situations in which an SLA's guarantees -- and penalties for failing to meet them -- don't apply. The list might include events such as natural disasters or terrorist acts. This section is sometimes referred to as a force majeure clause, which aims to excuse the service provider from events beyond its control.

Who needs a service-level agreement?

SLAs are thought to have originated with network service providers, but are now widely used in a range of IT-related fields. Companies that establish SLAs include IT service providers, managed service providers and cloud computing service providers. Corporate IT organizations, particularly those that have embraced IT service management (ITSM), enter SLAs with their in-house customers -- users in other departments within the enterprise. An IT department creates an SLA so that its services can be measured, justified and perhaps compared with those of outsourcing vendors.

2.3. Change Assessment

Why change is required in some system?

Changes are often implemented in an organization if something is not functioning correctly, or if production or quality is not at the expected level. After a change has been implemented, the organization needs to analyse and assess the change to determine if it has produced negative or positive results.

2.3.1. Possible Indicators for Assessing changes Maintenance procedures

- **Are equipment and infrastructure reliable?**
  - How many maintenance incidents were there per workstation/server during the current academic year (by cause, category, and location)?
  - What was the average number of downtime hours per workstation/server during the current academic year?
  - What is the average number of calls to help desk/tech-support services per workstation/server?

- What is the average elapsed time between the receipt of a call to the help desk and the response call to the end user?
- What is the average elapsed time between the initial response call and the notification of problem resolution?

➢ **Are appropriate preventive maintenance procedures in place?**

- Has a preventive maintenance schedule been established?
- Has a preventive maintenance checklist been provided to all end-users?
- Has access to frequently asked questions (FAQs) been provided to support staff and end users alike?
- Has access to user manuals been provided to end users?
- Are file backup procedures in place?
- Are disaster recovery procedures in place?

➢ **Are update and replacement procedures in place?**

- Has a replacement/upgrade schedule been established for hardware?
- Has a replacement/upgrade schedule been established for software?

➢ **Are diagnostic and repair resources available?**

- Is help desk support software available (e.g., trouble ticketing, resolution tracking)?
- Is diagnostic software available (as appropriate)?
- Are appropriate repair instruments/tools available on school premises?
- Are basic replacement parts in stock?

2.3.2. Establishing Maintenance Plans

Automobile manufacturers recommend having an engine tuned and oil changed regularly to keep a car running as efficiently as possible. Similar maintenance is required of a computer system. It is best not to wait until problems arise-avoid problems in the first place! An organization can carry out much of its own routine, preventive maintenance (e.g., checking database size, purging outdated records, and deleting idle user accounts), but in spite of efforts to deliver a high-quality preventive maintenance program, problems will still occur. To deal with them, many organizations have maintenance agreements with outside contractors for fix-it-when-it-breaks service, particularly for hardware. The key factors in these agreements are response time to a trouble call and the availability and proximity of spare parts. In other words, planners need to know how long it will take to get the problems fixed when (not if) they arise.

2.4. Design and implementation of improved maintenance procedure

When a maintenance program is successful, every area of the company is positively affected. Today, top organizations are reaping the benefits from implementing well- designed and managed reliability programs. By implementing the following things you can improve your maintenance procedures

Learn the 12 elements of effective reliability management. Be sure your organization understands these important elements and the impact they have on performance – starting at the very top. Without this leadership focus for your maintenance program, nothing else matters.

Track maintenance metrics. Using metrics and KPIs, maintenance organizations can efficiently manage maintenance activities and focus improvement initiatives on driving value.

Employ maintenance planning and scheduling. With effective planning, work can be completed with the least interruption to operations and the most efficient use of maintenance resources.

Consider an operator-driven reliability program. Without the ownership of your equipment in the operator's hands, it's difficult to be reliable. Using a well-planned approach involving all employees, equipment reliability will have a direct, positive impact on your bottom line.

Improve basic work systems. Many organizations spend too much time searching for new reliability and maintenance concepts, and very little time on implementing and improving what they just started.

Use joint reward systems to drive results. If an organization is serious about a closer integration between departments, the rewards systems must be designed to drive everybody's actions and performance toward the same goal and rewards.

Construct your maintenance plan. Creating a maintenance plan is generally not difficult to do. But creating a comprehensive maintenance program that is effective poses some interesting challenges. What makes the difference between an ordinary maintenance plan and a good, effective preventive maintenance program?

Listen to your equipment. Do you listen to your motors complaining about overload? Do you see your pump packing crying a flood? Do you hear your bearings whine about contaminated lubricants? Do you notice your steam system coughing excessive condensate and complaining about strained elbows?

Stop rewarding failure. Managers can talk all day about the organization's desire to be proactive, improve reliability, reduce costs, etc. But people don't pay attention to what you say; they pay attention to what you do. If you talk "reliability" but pay and recognize for failure, guess what you'll get? What gets rewarded gets done, period.

Target the 60 percent. On average, 30 percent of all preventive maintenance activities do not add value and should be eliminated. Another 30 percent of these activities could be replaced with condition-monitoring technologies and a predictive maintenance approach.

Go all-in with condition-based monitoring. There is little to no payback from using one or two condition- monitoring technologies – or applying CBM to a small amount of your assets and hoping it will evolve into a successful program.

More accurately estimate labour hours. Experience shows that the best labour estimates are routinely off as much as 100 percent. A job estimated to take five labour hours might take as many as 10 hours or as few as two.

Get the right leaders on-board. Corporate reliability leaders say that if they could do it over again, they'd spend more time choosing the right people for key leadership positions. With the right leadership in the right areas pushing the right things, you have success.

Employ a multi-tool approach for more savings. The preventive maintenance team at American Axle and Manufacturing addressed an issue found during a routine preventive maintenance work order using multiple condition monitoring tools.

Build a detailed and accurate equipment list. Despite what you may have heard, the foundation of a successful reliability program is a list – a detailed, accurate equipment list ideally recorded in your CMMS software. It contains the vital information you need to design, develop and engineer your maintenance program from the ground up.

Never accept "good enough". In a maintenance improvement process, there are several areas where there is always a desire or undercurrent to shortcut the process.

One of the most important actions of maintenance and reliability leadership is to expect and set the environment to allow the entire organization to practice "Good Enough Never Is" every day.

Improve work processes. Operating practices are a vital part of any preventive maintenance program. Good practices prevent failures. Poor practices encourage failures. This article discusses sample business practices that must be implemented to improve overall plant reliability.

Use the right predictive maintenance metrics. What gets measured gets improved. Or conversely, what doesn't get measured never will be improved. Tracking and reporting on key metrics lets you focus squarely on the behaviour changes you want.

Create a clear, concise vision. One of the first responsibilities of leadership is to provide a simple, clear view of what the future can and should look like. Having a clear, concise vision to improve your plant is important. This vision must be simple and visible.

Learn root cause analysis techniques. When a reliability problem arises, most organizations either address it at the symptomatic level or seek immediately to lay blame on a person or group. Root cause analysis is a systematic process for understanding and addressing the underlying causes of a problem.

Look, listen, feel, smell. Regardless of whether you're doing inspections with handheld computers or a paper system, can trend data or not, or have key performance indicators or not, you won't be successful unless your people can do quality inspections on equipment.

Decide on a lubrication staffing model. The question of who in an organization should be responsible for day-to-day machinery lubrication tasks is common. Learn the three most common organizational structures and create your own.

Create a planned backlog. The first maintenance scheduling principle is the prerequisite of having a planned backlog. Learn how to prepare and use a schedule as a control standard to improve maintenance productivity.

Use Reliability-centered Maintenance analysis. A Reliability-Centered Maintenance analysis should be viewed as a serious exercise for your business. An RCM analysis is an investment that takes time, resources and money to complete, but is worth the effort.

Implement Total Productive Maintenance in 12 steps. Implementing TPM using these 12 steps will start you on the road to "zero breakdowns" and "zero defects." Achieving 100 percent reliability takes discipline and teamwork.

Break out of maintenance budget jail. If you are in budget jail and have tried to get out by preaching reliability to the people above you but have made little headway, here is a plan to break you out.

Learn the value of "P". Point P on the P-F Curve is where a defect enters a machine. At some time in the future, this will cause a functional loss of some kind. As a defect lingers in a machine, the machine functionality decreases over time. At some point in the future, Point F, total failure of the machine occurs.

Create an equipment bill of materials. An equipment bill of material lists all the components of an asset, including its assemblies and subassemblies. With a reliable equipment bill of materials, a planner can determine exactly what parts are needed. And in an emergency, it provides valuable information to craftsmen and others to ensure that the right parts are identified and procured.

Use P-F intervals to map and avert failures. The P-F interval is a valuable piece of information for any maintenance team, and you don't need special education to use it. The use of P-F intervals in determining the right maintenance to perform at the right time need not be confined to RCM.

Consider a continuous monitoring system. Continuous monitoring is the application of dedicated devices for collecting predictive maintenance-style data to aid in a condition monitoring program. With each passing year, this technology gets cheaper, and the desire for more complex and more robust monitoring gets larger.

Build a strong relationship with operations. To get better at maintenance, you must get better at building a positive relationship with operations. To achieve maintenance excellence, you must have an excellent relationship. This means having maintenance in full alignment with the larger goals of your operations and your company.

Quantify the cost of a functional failure mode. What is the real cost of a failure? Unfortunately, we don't know until after the failure has occurred - and reliability is about avoiding the failure.

Develop standard maintenance procedures. Plants often fail to see the importance of having well-written procedures for most tasks. This article discusses the importance of having good procedures and presents the details needed to develop well-written standard maintenance procedures.

Manage assets by criticality. Through proper construction of the criticality analysis model, reliability engineering will be able to illustrate what reliability enhancements must be made to manage criticality, thus improving their ability to manage assets by criticality.

Teach operators the "Should-Actual Five-Whys" method. Operators in a reliability-focused culture should have a questioning attitude and be very observant. The inclusion of the S-A-5Whys tool in their skill set will benefit the organization by the early identification and resolution of problems, leading to increased asset reliability.

Get more out of your EAM. All EAM systems contain the same basic capabilities in support of your maintenance program. They are like any other software package – their success depends on how they are implemented and, more importantly, how they are used.

Optimize outages with effective task planning. Outages can have elaborate schedules, but often are unsuccessful due to ineffective advanced planning, which results in inefficient work execution and outage schedule overruns. Outages can only be successful when the outage work is planned effectively before the work is scheduled and/or started.

Put multiple CBM tools to use. It is essential to understand how equipment performs in a facility and to be able to predict and prevent failures before they happen. The results of the combination of condition-based monitoring technologies will give the reliability engineer an even greater confidence when communicating to management when an asset is approaching an impending failure.

Apply the correct maintenance strategies. True reliability is achieved when the most cost-effective methods are applied to the assets in your plant, thereby maximizing reliability with the minimum total cost to the business.

Benchmark your lubrication program. Benchmarking provides a much-needed scorecard for areas of lubrication that may not be obvious or often considered for improvement. It is true that we “don’t know what we don’t know”.

Detect machine problems early. This massive list of inspection items will allow you to detect problems early, and hopefully eliminate downtime and/or reduce maintenance costs.

Remove process bottlenecks. If your process bottlenecks are linked closely to the maintenance and reliability of your equipment, it is most likely you have a highly reactive maintenance organization. To move from a primarily reactive regime, significant focus must be placed on developing and deploying systems that move the organization toward being proactive.

Optimize PM tasks. Unfortunately, most preventive maintenance tasks lack the detail that will provide quantitative data for equipment history, and they are written without considering failure modes. The solution is to practice Preventive Maintenance Optimization (PMO), using all aspects to write PM procedures that are value added, comprehensive, repeatable, organized, and specify a correct duration and interval of execution.

Create a lean and effective oil analysis program. Oil analysis is a powerful tool in a maintenance program. This case study presents alternatives to expensive in-house test equipment, good utilization of outside labs, oil storage solutions, methods of reporting findings to further the program, and selling the program to upper management as well as to operations and maintenance.

Put maintenance checklists to use. While most groups will say they have checklists, requiring their use and the accountability are often major factors for success. In your organization, what processes do you have in place to ensure that people use maintenance procedures and checklists?

Avoid the 5 biggest risks. Asset management is an integrated approach to optimizing the life cycle of your assets, beginning at conceptual design, through to usage, decommissioning and disposal. By acknowledging and paying attention to these five primary risks to effective asset management, you can put in place plans to mitigate the effects these might have on their program.

Give maintenance technicians equipment ownership. How do you strike a balance between equipment ownership and building the skills through cross training, and having the ability to get the work done all the time? Is it based on the culture of the organization?

Be smart about kitting. Kitting for maintenance crafts to perform their tasks is one of the easier and more effective ways to allow quality completion of the job with minimal productivity impact, especially when accompanied by a well-planned and functionally scheduled job.

Work towards zero failures. Experiences and data show that zero failures are possible in a maintenance program. As someone once said, “If you think you can’t, you’re probably right. If you think you can, you’re probably right.”

Manage the change process. The most difficult but most beneficial aspect of leading a maintenance and reliability improvement effort is managing the change process in organizations. The behaviour change process from a reactive state to a proactive state is a challenging transition for any maintenance program.

Self-Check 2	Written Test

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write **True** if the statement is **Correct** and **False** if the statement is **Incorrect**

1. The Monitoring Maintenance Lifecycle is a monitoring development process to reduce maintenance costs.
2. Monitoring Maintenance Lifecycle are methods and standards for improving and mastering maintenance processes.
3. Maintenance Lifecycle is based on bone fish model.
4. Changes are often implemented in an organization if something is functioning correctly.
5. After assessment is take place the next step will be analysis

II. Choose the best answer

1. One of the following is Possible Indicators for Assessing changes Maintenance procedures

A. Are equipment and infrastructure reliable?
B. Are appropriate preventive maintenance procedures in place?
C. Are update and replacement procedures in place?
D. All

III. Explain the Following

1. Apply the correct maintenance strategies

2. Remove process bottlenecks

3. Optimize PM tasks

Unit Three: IT system components maintenance

This unit to provide you the necessary information regarding the following content coverage and topics:

- Identification of warranty status
- System architecture and configuration
- Critical components and document recommendations

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Determine and documenting Warranty status
- Review System architecture and configuration documentation
- Identify Critical components and document recommendations

3.1. Identification of warranty status

- **General:** Legally binding assurance (which may or may not be in writing) that a good or service is, among other things, fit for use as represented, free from defective material and workmanship, meets statutory and/or other specifications. A warranty describes the conditions under, and period during, which the producer or vendor will repair, replace, or other compensate for, the defective item without cost to the buyer or user. Often it also delineates the rights and obligations of both parties in case of a claim or dispute.
- **Contracting:** Expressed or implied undertaking that a certain fact regarding the subject matter of a contract is, or will be, true.

Unlike conditions (the central points), warranties are deemed incidental points, and a breach of warranty is usually not a valid reason for voiding a contract but it entitles the aggrieved party to damages. See also in nominate term and intermediate term.

- **Insurance:** Written pledge by the insured party that a specified condition exists or does not exist. Breach of warranty entitles the insurer to treat the insurance contract as void even if the actual loss is unaffected by the breach. See also representation.

ICT equipment companies guarantees that all the products undergo backbreaking quality control testing before delivery and installation. In the event that any product of these manufacturers is found to be defective, the company will provide service for product repair and/or component replacement as may be necessary within the warranty period as per the terms mentioned here under.

3.2. System architecture and configuration

Give general description of the system, from the point of the user:

- In what environment it works (home, near patient bed, operating rooms….)
- Who the users are
- What it is for
- The main functions
- The main interfaces, input and outputs

If your software is integrated in a large system, you may reference a document that describes this system.

Physical architecture overview

Describe the hardware components on which software runs and their interactions/relationships

Use components diagrams, deployment diagrams, network diagrams, interface diagrams…

Hardware Component description

Describe the content of each hardware component in the architecture

- Its identification
- The purpose of the component
- The software component it receives
- Its technical characteristics: type of machine, CPU, RAM, disk and so on.
- Its network hardware interfaces

Logical architecture overview

- Describe the top level software components and their interactions/relationships.
- Use UML package diagrams and/or layer diagrams and/or interface diagrams.
- Describe also the operating systems on which the software runs.

Software Component description

Describe the content of each top-level software component in the architecture the description should contain:

- Its identification
- The purpose of the component,
- Its interfaces with other components,

- Its network interfaces,

The hardware resources it uses, for example: average RAM usage, peak RAM usage and peak frequency and duration, disk space for permanent data, disk space for cache data, average CPU usage, peak CPU usage and peak frequency and duration …

- Software SOUP

If you use SOUP (Software of Unknown Provenance), list them here. For each SOUP, describe:

- Its identification and version
- Its purpose
- Where it comes from: manufacturer, vendor, university …
- Whether it is maintained by a third party or not If this is an executable,
- What are the hardware / software resources it uses
- Whether it is insulated in the architecture and why
- Its interfaces and data flows
- Which SOUP functions the software uses
- How the SOUP is integrated in the software
- What hardware/software resources it requires for proper use

Note: have a look at FDA Guidance « Off-The-Shelf Software Use in Medical Devices » to determine if you need specific or special documentation for your COTS.

If there is a list of known bugs on your COTS, you may add here this list with a review of their consequences in terms of software failure and patient safety. If there are concerns about known bugs, they should be treated by the risk analysis process.

3.2.1. Dynamic behaviour of architecture

The architecture was designed to answer to functional requirements.

For each main function of the system, add a description of the sequences / data flow that occur.

Use sequence diagrams, collaboration diagrams

Workflow / Sequence 1

Describe here the workflow / sequence of a main function

For example, the user queries data, what happens, from his terminal to the database?

Workflow / Sequence 2

Repeat the pattern for each main function of the system

3.2.2. System architecture capabilities

Describe here the rationale of the hardware / software architecture in terms of capabilities:

- Performances (for example response time, user mobility, data storage, or any functional performance which has an impact on architecture)
- User / patient safety
- Protection against misuse
- Maintenance (cold maintenance or hot maintenance),
- Adaptability, flexibility
- Scalability, availability
- Backup and restore
- Hardware and Software security: fault tolerance, redundancy, emergency stop, recovery after crash …
- Administration,
- Monitoring, audit
- Internationalization

3.2.3. Network architecture capabilities

If the medical device uses/has a network, describe here the rationale of the hardware / network architecture:

- Bandwidth
- Network failures
- Loss of data
- Inconsistent data
- Inconsistent timing of data
- Cyber security (see FDA Guidance on Cyber Security of networked medical devices)

Risk analysis outputs

If the results of risk analysis have an impact on the architecture, describe here for each risk analysis output what has been done to mitigate the risk in the architecture.

Use diagrams if necessary, like architecture before risk mitigation and architecture after risk mitigation, to explain the choices.

Human factors engineering outputs

If the results of human factors analysis have an impact on the architecture, describe here for each risk human factors output what has been done to mitigate the risk in the architecture.

3.3. Critical components and document recommendations

3.3.1. Definition of Critical Components

Critical Components means a component or system of components that, due to their importance in the continued proper operation of the device, have been designated by the manufacturer as requiring special fabrication, maintenance, inspection or operation. To document recommendations first of all we must identify the critical components and software from the followings.

- **Computer hardware**

This is the physical technology that works with information. Hardware can be as small as a smart phone that fits in a pocket or as large as a supercomputer that fills a building. Hardware also includes the peripheral devices that work with computers, such as keyboards, external disk drives, and routers. With the rise of the Internet of things, in which anything from home appliances to cars to clothes will be able to receive and transmit data, sensors that interact with computers are permeating the human environment.

- **Computer software**

The hardware needs to know what to do, and that is the role of software. Software can be divided into two types: system software and application software. The primary piece of system software is the operating system, such as Windows or iOS, which manages the hardware’s operation. Application software is designed for specific tasks, such as handling a spreadsheet, creating a document, or designing a Web page.

- **Telecommunications**

This component connects the hardware together to form a network. Connections can be through wires, such as Ethernet cables or fibber optics, or wireless, such as through Wi- Fi. A network can be designed to tie together computers in a specific area, such as an office or a school, through a local area network (LAN). If computers are more dispersed, the network is called a wide area network (WAN). The Internet itself can be considered a network of network.

Self-Check 3	Written Test

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Write True if the statement is Correct and False if the statement is Incorrect

1. A warranty describes the conditions under, and period during, which the producer or vendor will repair or replace defective item without cost to the buyer or user.
2. ICT equipment companies guarantees that all the products undergo backbreaking quality control testing before delivery and installation.
3. Pledge by the insured party that a specified condition exists or does not exist

II. Choose the best answer

1. One of the following is the capability of computer architecture

A. Bandwidth

B. Inconsistent Data

C. Cyber security

D. All

III. Fill the blank

1. _____Describe the hardware components on which software runs and their interactions/relationships.
2. _____Describe the content of each hardware component in the architecture.
3. _____Describe the top level software components and their interactions/relationships.

Unit Four: Maintenance procedures

This unit to provide you the necessary information regarding the following content coverage and topics:

- Preventative maintenance
- Maintenance procedure
- Documentation of Recommended Procedure
- Staff orientation about maintenance
- OHS

This guide will also assist you to attain the learning outcomes stated in the cover page. Specifically, upon completion of this learning guide, you will be able to:

- Create Preventative maintenance schedule
- Identify and Applying maintenance procedure
- Document Recommended procedure and submitting for approval
- Give Orientation to implementing staffs and follow up maintenance schedule
- Observe OHS throughout the process

4.1. Preventative maintenance

Preventive maintenance is a regular and systematic inspection, cleaning, and replacement of worn parts, materials, and systems.

Purpose of preventive maintenance

Reduce the likelihood of hardware or software problems by systematically and periodically checking hardware and software to ensure proper operation. Reduce computer down time and repair costs

Troubleshooting is a systematic approach to locating the cause of a fault in a computer system.

- Troubleshooting is a learned skill.

- Not all troubleshooting processes are the same, and technicians tend to refine their own troubleshooting skills based on knowledge and personal experience.

- **Hardware Maintenance**

Make sure that the hardware is operating properly.

- Check the condition of parts.
- Repair or replace worn parts.
- Keep components clean.
- Create a hardware maintenance program.

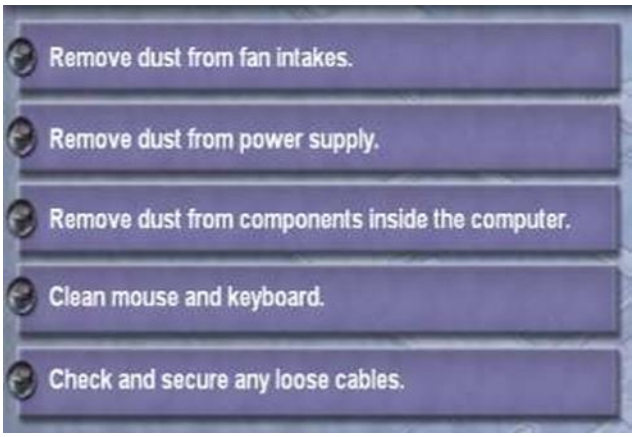


Fig 1.1.Hard ware maintenance

- **Software Maintenance**

- Review updates
- Follow policies of your organization
- Create a schedule



Fig 1.2. Software maintenance

Preventive Maintenance Benefit

- Reduce computer down time.
- Reduce repair costs.
- Reduce loss of worker productivity.

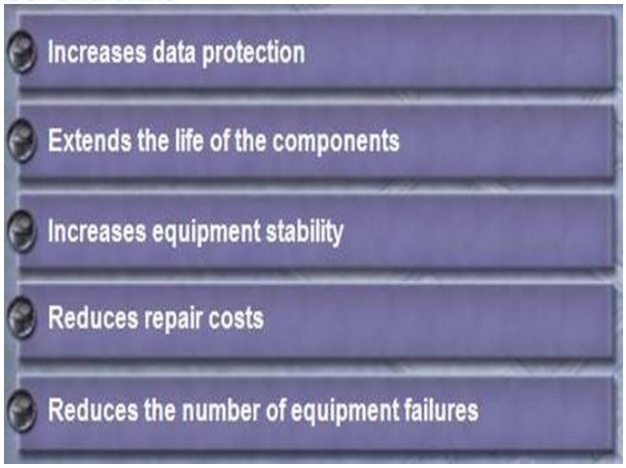


Fig 1.3. Preventive maintenance

The Troubleshooting Process

- Follow an organized and logical procedure.
- Address possible issues one at a time.
- Troubleshooting is a skill that is refined over time.
- The first and last steps involve effectively communicating with the customer.



Fig 1.4. Troubleshooting

Data Protection

Check with customer

- Date of the last backup
- Contents of the backup
- Data integrity of the backup
- Availability of media for data restore

If no backup can be created, ask customer to sign a release form

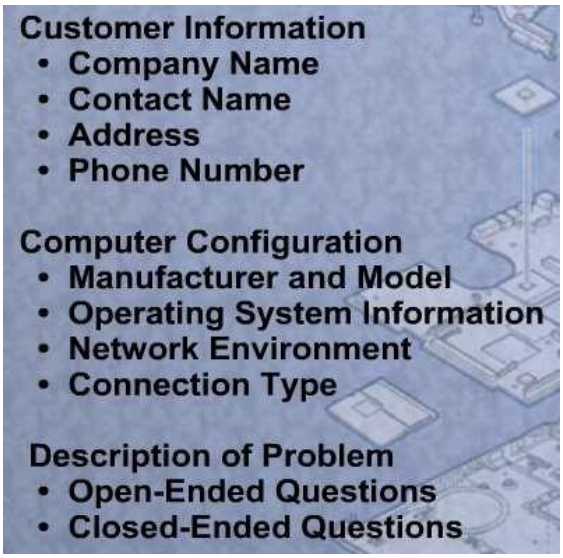


Fig 1.5. Data protection

Gather Data from the Customer

- Communicate respectfully with the customer
- Start with open-ended questions

"What types of problems are you having with your computer or network?"

- then, ask closed-ended (yes/no) questions "Have you changed your password recently?"

Verify Obvious Issues

- Problem may be simpler than the customer thinks.
- checking for obvious issues can save time.
- If this step turns up nothing, continue to the next step of the troubleshooting process.

Try Quick Solutions

- May provide additional information,

  Even if they do not solve the problem.
- Document each solution you try.
- May need to gather more information

  From the customer.
- If you find the problem at this stage,

Document it and proceed to the end of the troubleshooting process.

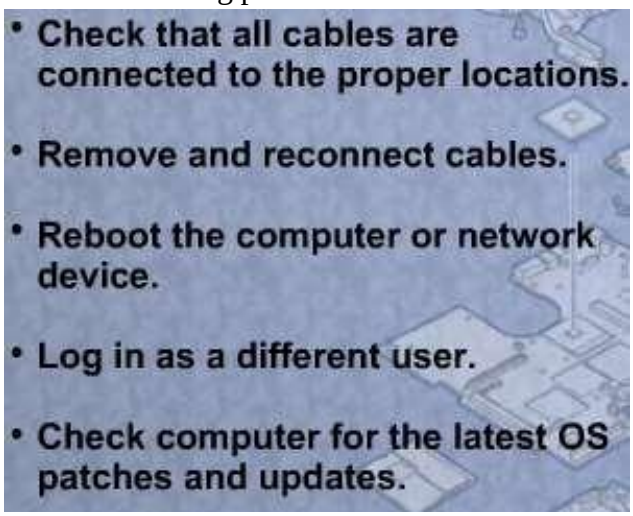


Fig 1.6. Solution

Gather Data from the Computer

 When system, user, or software errors occur on a computer, the Event Viewer is updated with information about the errors:

- What problem occurred?
- The date and time of the problem
- The severity of the problem
- The source of the problem
- Event ID number
- Which user was logged in when the problem occurred?

 Although this utility lists details about the error, you may still need to research the solution.

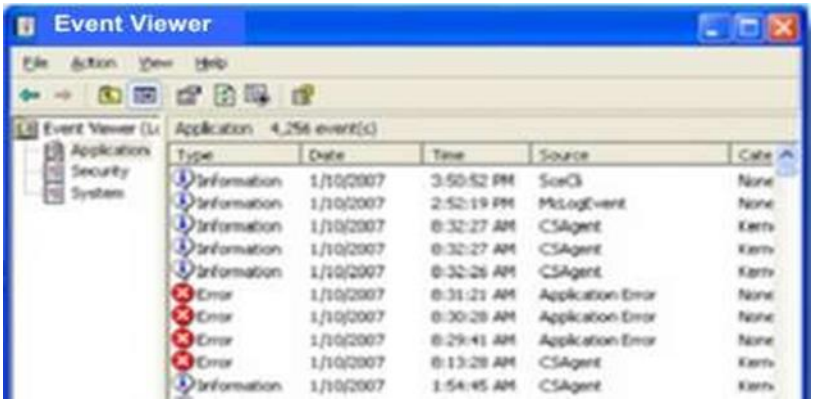


Fig 1.7. Event viewer window

Gather Data from the Computer Device Manager

 A flag of! Indicates the device is acting incorrectly.

 A flag of X indicates the device is disabled.



Fig 1.8. Event viewer

Gather Data from the Computer

 when troubleshooting, power on the computer and listen to the beep code sequence. Document the beep code sequence and research the code to determine the specific hardware failure.

 If the computer boots and stops after the POST, investigate the BIOS settings to determine where to find the problem. Refer to the motherboard manual to make sure that the BIOS settings are accurate.

 Conduct research to find software to use to diagnose and solve problems. Often, manufacturers of system hardware provide diagnostic tools of their own.

Evaluate the Problem, Implement the Solution

 Research possible solutions:

 Prioritize solutions to try.

 Try easiest solutions first.

 after an unsuccessful try, undo any changes you have made.

Unnecessary changes could complicate finding the solution



Fig 1.9. Problem solving

Close with the Customer

 Discuss the solution with the customer

 Have the customer confirm that the problem has been solved

 Document the process

- Regular preventive maintenance reduces hardware and software problems.
- Before beginning any repair, back up the data on a computer.
- The troubleshooting process is a guideline to help you solve computer problems in an efficient manner.

Document everything that you try, even if it fails. The documentation that you create will become a useful resource for you and other technicians.

4.2. Maintenance procedure

4.2.1. Type of Maintenance

❖ Reactive maintenance (breakdown maintenance)

Also known as breakdown or run-to-failure, reactive maintenance is pretty simple: fix things when they break. Since repairs are not planned, it's a good method to employ for equipment that is not essential for operations or has a low cost (think anything that's rarely used or duplicates the function of other equipment).

For example, think of a $1000 belt feeder, whose lifetime value can be extended by 10% by servicing it every 3 months. How hard are you willing to work to save $100? For a non-critical piece of machinery, the answer should be "not hard"."

While it requires minimal planning, the drawbacks of reactive maintenance can be substantial if it's not carried out correctly. If the approach is used for all equipment, there can be huge delays in production when a critical piece of equipment fails. Further, if you don't have the right parts and supplies on hand, the costs for rushed shipping can become significant. In short, reactive maintenance often means more downtime and higher maintenance costs when it's not used strategically.

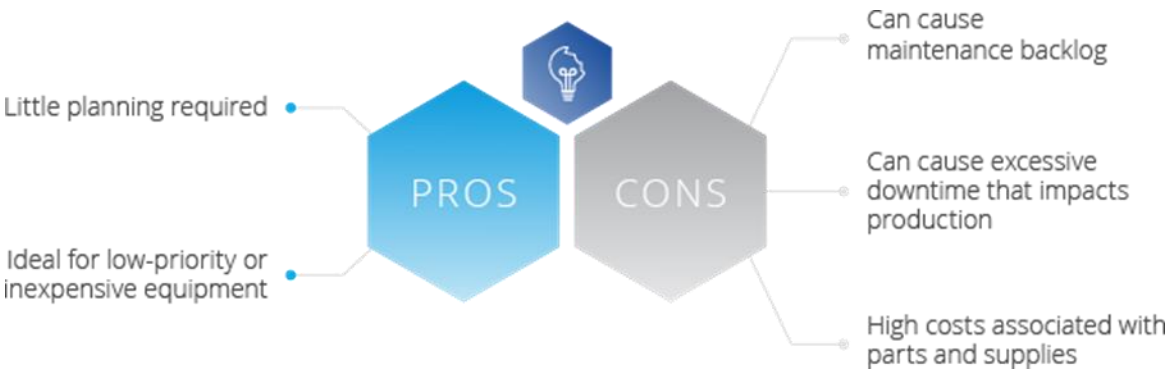


Fig 1.9 Reactive maintenance

❖ Preventive maintenance (scheduled)

Also known as proactive maintenance, this method involves periodically taking assets offline and inspecting or repairing them at predetermined intervals (usually time or event-based triggers). The goal of this approach is to extend the useful life of an asset and prevent breakdowns from occurring.

Many organizations employing preventive maintenance use CMMS software to trigger work orders when a PM is due. This allows a facility to automate much of its scheduling efforts, which is a key ingredient of this preventive approach. Because planning is done in advance, it's much easier to have the right parts and resources on hand to complete each task.

With all maintenance types, there are potential drawbacks to relying solely on preventive maintenance. If the PM schedule isn't regularly monitored, audited, and improved, "PM creep" can occur. This is when technicians get bogged down by unnecessary tasks and cost the organization time and money.

Similarly, performing too many PMs can open the door for post-PM breakdowns. There are a number of ways to prevent this, but the risk gets higher as PMs Get more frequent. The bottom line is, if a preventive maintenance program is used, it should go hand in hand with PM optimization.



Fig 1.10.Preventive maintenance

- **Predictive maintenance (PdM)**

Predictive maintenance (PdM) aims to predict failures before they happen so maintenance can occur at just the right time. PdM uses data from machine sensors and smart technology to alert the maintenance team when a piece of equipment is at risk of failing. For example, a sensor may use vibration analysis to alert the maintenance team that a piece of equipment is at risk of failing, at which point it will be taken offline, inspected, and repaired accordingly.

It is possible to carry out PdM via visual inspections of equipment, but the easiest way to establish a predictive maintenance strategy is by using a CMMS to track meter readings. The advantage of PdM (over PM) is the potential for cost savings from reduced man-hours spent on maintenance, and more insight as to the performance and potential issues arising with the machine. Additionally, a reliance on data and sensor information means maintenance is determined by the actual condition of equipment, rather than a best-guess schedule or gut feel.

Of course, relying so heavily on data means that there is a higher up-front cost to ensuring this maintenance approach can thrive. Another thing to keep in mind with predictive maintenance is that you have to walk before you can run. For an organization coming from a pen-and-paper or Excel- based maintenance program, you have to first build on the processes and insights that preventive maintenance provides in order to build an effective predictive maintenance plan.



Fig 1.11. Predictive maintenance

- **Reliability-centered maintenance (RCM)**

Reliability-centered maintenance (RCM) addresses the fact that failure is not always linear. RCM is a highly-involved process that seeks to analyse all the possible failure modes for each piece of equipment and customize a maintenance plan for each individual machine. The ultimate goal of RCM is to increase equipment availability or reliability.

RCM is considered complex because each individual asset must be analysed and prioritized based on criticality. The most critical assets are those that are likely to fail often or will result in large consequences in the event of failure. Because each piece of equipment is analysed on its own, it's possible that the end result of embarking on an RCM effort is having as many different maintenance plans as you do pieces of equipment.

RCM is very sophisticated, to the extent where it is not a realistic or necessary technique for every organization. It's requires a very mature maintenance team that has mastered prevention, basic inspections, predictive maintenance, and has access to lots of existing data on their assets.

4.3. Documentation and Approval of Recommended Procedure

Document approvals are formalized processes that you use to track the development of a whole document. Using document approvals, you can route documents for approval, monitor the approval process from person to person, log who approved or denied the document, and review suggestions that they made about the document. The process facilitates a more detailed control of a document and helps ensure that the contract is within standards of individuals and groups in an organization.

Supplier Contract Management provides a sample approval process definition as a starting template process for the document and the clause approval workflow processing. Application administrators can define approval framework configurations to support an organization's internal processes.

Document approvals use approval framework. For document approvals, the approval process ID that you use must be named Document. The approval framework supports multiple approvers who can be notified at the same time, creating parallel approval paths. Approvers can approve or deny transactions and assign ad hoc reviewers or approvers for the transaction. When the approval process is complete, the system updates the document as approved or rejected. Supplier Contract Management also incorporates an optional clause-level approval stage so that the system can automatically include appropriate individuals in an approval process based on the presence or modification of specific contract clauses.

During the approval process, approvers can add other approvers or reviewers to the current or a later stage of the approval process. For example, if an author wants input from an inventory analyst, she can add the analyst as an approver. This is called ad hoc approval. It applies only to the approval instance in which the addition occurs and does not affect the overall approval flow. Only the approver who adds an ad hoc approval can delete it.

An author can also be a document approver. Document writers approving their own documents are called self-approval. A check box setting on the Approval Process Definition page enables self- approval. If self-approval is enabled, the author's approval is assumed and the process continues; however, you can establish criteria that help control the author's approval authority. For example, you can place a limit on the monetary amount for which the author writes a document so that if the transaction is over that amount, the author cannot be an approver.

An administrator can manage approvals by reassigning those that do not have alternates defined for their approval. You can enter criteria to limit the number of approvals that the system displays.

The approval processing of documents can also include enabling internal users to digitally sign documents at the same time they approve the document if the installation and document type

settings dictates signatures are to be captured for this document during approvals. You can configure the system to capture internal signatures before, during, or after approvals.

Preview Approval

Select to view a list of approvers based on the approval process definition.

Submit for Approval

Select to immediately start the approval process. After starting the approval process, the system displays another Document Approval Status page with the new approval status. Using the page you can:

- Review approvers and reviewers.
- Review approval process stages and paths.
- Make comments about the document before continuing the approval process.
- Add approvers and reviewers.
- Start new approval paths.
- Cancel the approval process.

4.4. Staff orientation about maintenance

Why is Orientation Important?

Orientation is important because it lays a foundation for the users in the department. First impressions are important since they establish the basis for everything that follows. Without orientation, users sometimes feel uncomfortable in his/her activities and take longer to reach his/her full potential.

Orientation is important because it:

- Provides the users with concise and accurate information to make him/her more comfortable in the job;
- Encourages users confidence and helps the new user adapt faster to the job;
- Contributes to a more effective, productive workforce;
- Improves users retention; and
- Promotes communication between the technical person and the users.

4.5. OHS

4.5.1. Overview of OHS

For smooth, safe and successful maintenance work a prior risk assessment has to be carried out. A risk assessment is a careful examination of what could cause harm to people, allowing one to judge whether there are enough precautions in place or more if more are needed to prevent harm. It involves identifying the hazards present in any undertaking (whether arising from work activities or from other factors, e.g. the layout of the premises) and then evaluating the extent of the risks involved, taking into account existing precautions Potential hazards could be: dangerous substances, confined spaces, working at height, awkward positions, plant under pressure, moving parts of machinery, unexpected start-ups, chemical substances or dust in the air, stress, communication problems, etc. Outsourcing and subcontracting should be afforded special consideration and the risk assessment should include both perspectives as well as any problems with work arrangements and communication.

The results of a suitable and sufficient risk assessment should enable to choose which good practice measures are most appropriate in preventing risks in general and also in preventing risks to any individuals identified as being particularly at risk. The implementation may mean making changes to the organization and working procedures, working environment, equipment and products used. Changes could also be necessary in training management and staff as well as improving communications.

Employees and their representatives should be involved in the carefully planned adoption of any policies and measures, as a key component of success. This should include coordination and communication between the contractor and service company personnel. The general principle, also laid down by the respective EU directives, is that risks should be prevented at source and that work organization, tasks, equipment and tools should be adapted to workers in order to eliminate and reduce risks. Measures should follow the prevention hierarchy:

- Elimination of risks
- Substitution e.g. of dangerous substances
- Collective control measures like exhaust systems
- Individual control like personal protective equipment

This means for example that personal protective equipment has only to be seen as last resort. There have to be periodic reviews to check that measures, policies and procedures remain appropriate and are working and revised if necessary.

Special issues, qualification

Based on the conducted risk assessment the following issues need special attention:

- A qualification level has to be determined for the specific repair and maintenance tasks. It may be necessary to put a permission system in place, only giving specifically trained people access to sensitive and dangerous areas. The issuing of permits for work and lock-off systems has also to be considered. A permit to work should detail the work to be done and the precautions to be taken.
- Enough time and appropriate resources have to be allocated. Stress and unsuitable tools may lead to errors, unsafe situations and prolonged down times.
- Coordinating panels involving the service company have to be set up while the means and paths of communication between all stakeholders need to be established carefully. Comprehensive instructions should be provided. For complicated tasks written work orders should be issued and discussed with the workers.

Ensuring instructions, qualification and further education of the workers performing maintenance tasks is another important planning issue. With buildings and machines becoming more and more sophisticated, and maintenance also being seen as a means to improve technology, maintenance staffs need to keep up with this development. Employees should be given the opportunity to not only develop their knowledge but to also bring in their experience. This is all the more important as maintenance tasks can always bring about situations of unplanned and unforeseeable danger and workers need to make use of all their knowledge and skills to manage these situations safely. It also plays an important role in changing risky behaviour on behalf of the workers. However, in this aspect it is also of utmost importance that all superiors set a good example and always follow the determined rules themselves.

It might also be necessary to seek advice from outside experts, if the company does not have sufficiently qualified personnel.

Maintenance workers and their representatives should already in the planning stage look to it, that the outsourcing issue is considered sufficiently:

- Outside workers are usually less familiar with the company-specific layout and construction of machinery and plants; special instructions are needed.
- Communication between own and outside workers may be problematic with regards to time, language and organisation; special monitoring as to understanding of measures is necessary.
- Coordination of production and maintenance work becomes more difficult; contact persons, deputies have to be identified and time schedules set up to ensure they are on site during the maintenance work.

Providing a safe work area

Only authorized personnel should be allowed to do repair or maintenance work. This becomes all the more important when the machines and structures are more sophisticated. Only then can it be guaranteed that the right steps are followed and the correct equipment is used.

The work area needs to be secured by preventing unauthorized access, for example, by using barriers and signs and safe routes, which have to be established for workers to enter and exit the work area.

Structures and machines have to be cut off from any energy sources, such as power supplies and pressure hoses using special locks, whereby only the maintenance workers and their supervisors have the keys necessary for doing this. Warning signs should be attached to machinery, with the date and time of lock-off, as well as the name of the person authorized to remove the lock. In this way, the safety of the worker performing the maintenance on the machine will not be jeopardized by another worker inadvertently starting it up.

Any residual energy should be safely discharged (e.g. an exhaust system for decompression of gases and liquids may be necessary) and it should be considered that some machine parts may need additional time to move into their home position. This has to be indicated in the machine's manual. The essential health and safety requirements of machines and plants have to be met with regards to maintenance. They have been established by the Council Directive 2006/42/EC on machinery.

Sometimes, it can be necessary to conduct the repair or maintenance work at running machines. In this case special measures have to be taken:

- The normal safeguards should be in place and should be used.
- If that is not possible, special protection devices have to be used (special tools, mobile switches), the speed of the machine has to be reduced, and special covers for dangerous areas have to be provided.
- If this should, in some very special cases, not be possible, special measures have to be taken based on a detailed risk assessment. Supervision must be provided throughout the process.

Allocating appropriate equipment

According to statistical data, the next largest cause of accidents during maintenance – after „getting injured at running machines" – is, „falling from heights". This clearly shows that in addition to improving the design of structures, machines and plants in order to provide easier access for maintenance and repair, it is very important that maintenance workers have safe access to and safe work platforms at their place of work. Ranked in hierarchical order, the following measures are recommended:

- Stationary steps (fitted with slip resistant material) and work platforms with guards (secured against unauthorized access)
- Scaffolds (providing proper stability and structural safety)
- Mobile elevating work platforms
- Properly installable special work platforms for specific fork lifts
- Safety ladders (if possible, fitted with special working platforms)
- Personal protection equipment against falling.

Maintenance work often requires contact with a variety of substances, many of them hazardous:

- Cleaning and lubricating agents should be selected carefully e.g. using selection tools such as GISBAU CatSub or Clean tool, in order to use substances with the least impact on human health.
- During the work time, gases, smokes and vapors may occur, e.g. by releasing pressure, cleaning surfaces or welding and soldering. When appropriate, quantitative measurements should be taken. Workers or supervisors can also be equipped with test tubes. Appropriate exhaust systems have to be put in place and comfortable personal protection equipment has to be provided.
- If liquids flowing from machines or plants cannot be avoided during maintenance work, workers have to have proper instructions and equipment to handle these (exhaust, skin protection, etc.).
- Work often produces or raises dust. The risk assessment will indicate as to whether there is any asbestos risk present (brake linings, sealing, insulations). In this case, very special measures have to take.
- Flammable substances as well as welding and soldering will also involve the danger of fires and explosions. (Dust too, when getting airborne, can lead to explosions). This requires special equipment (e.g. non-sparking tools) and related instructions.

Self-Check 4	Written Test

Name: _____ Date: _____

Instruction: Answer all the questions listed below, if you have some clarifications- feel free to ask your teacher.

I. Choose the correct answers from the given alternatives

1. Event Viewer is holds:

A. What problem occurred
C. The severity of the problem
B. The date and time of the problem
D. All

2. The Troubleshooting Process

A. Follow an organized and logical procedure.
B. Address possible issues one at a time.
C. Troubleshooting is a skill that is refined over time.
D. All

3. Which one is not Preventive Maintenance Benefits

A. Increase equipment stability
B. Decreases life time of the components
C. Increase Data protection
D. All

4. In a Device Manager A flag of "!" indicates the device is

A. Working Correctly
B. Installed and functional
C. Acting incorrectly
D. All

II. Write True if the statement is True and Write False if the statement is incorrect

1. Predictive maintenance aims to predict failures before they happen so maintenance can occur at just the right time.
2. RCM is very sophisticated, to the extent where it is not a realistic or necessary technique for every organization
3. Predictive Can be expensive to set up
4. Reactive maintenance often means more downtime and higher maintenance costs when it's not used strategically.

III. **Fill the blank**

1. _____Document approvals are formalized processes that you use to track the development of a whole document.

References

1. **Schuh, G., Lorenz, B., „TPM – eine Basis für die wertorientierte Instandhaltung„, Betriebliche Instandhaltung, Springer Verlag, Berlin Heidelberg, 2009.**
2. **European Agency for Safety and Health at Work (2011), Risk assessment. Retrieved 24 February 2011, from:**
3. **Schuh, G., Lorenz, B., „TPM – eine Basis für die wertorientierte Instandhaltung„, Betriebliche Instandhaltung, Springer Verlag, Berlin Heidelberg, 2009.**
4. **VMBG – Vereinigung der Metallberufsgenossenschaften, „Instandhaltung – schnell aber sicher„, Mitteilungsblatt Gesund+Sicher, Juni 2001.**
5. **EU-OSHA – European Agency for Safety and Health at Work (2011), Risk assessment. Retrieved 24 February 2011, from:**
6. **Schuh, G., Lorenz, B., „TPM – eine Basis für die wertorientierte Instandhaltung„, Betriebliche Instandhaltung, Springer Verlag, Berlin Heidelberg, 2009.**
7. **http://www.micro2000.com/**
8. **http://www.protechdiagnostics.com**
9. **IBM Launches World‘s First Desktop PC with 100% Recycled Plastic Resin, 1 March 1999.**
10. **http://www.ibm.com/ibm/environment/news/epro.shtml. 10 IBM Corporate Responsibility Report 2006.**
11. **http://www.ibm.com/ibm/responsibility/pdfs/IBM_CorpResp_2006.pdf.**

Participants of this Module (training material) preparation

No	Name	Qualification (Level)	Field of Study	Organization/ Institution	Mobile number	E-mail
1	ZERIHUN ABATE	A (MSC)	IT	Sabata Poly_technic College	0911858358	Zedoabata2017@gmail.com
2	MICHAEL KASSHUN	B (BSC)	IT	Misrak Poly_technic College	0989308914	Miko3mt@gmail.com
3	SEWAYEHU W/YOHANNES	A (MSC)	IT	Sodo Poly_technic College	0911716733	Sewnet1221@gmail.com
4	YONAS BEYANE	A (MSC)	IT	EthioItaly Poly_technic College	0915007456	yonas.beyane@gmail.com
5	ABEBE MULATU	B (BSC)	IT	Daye Poly_technic College	0904834788	abebemulatumgh@gmail.com
6	SOLOMON YILMA	A (MSC)	IT	APTC (ASSOSA)	0911954729	sollangano@gmail.com
7	YOHANNES BEKELE	B (BSC)	CS	Hawassa (HPTC)	0939497218	Ybekele71@gmail.com
8	TEWDROS GIRMA	A (MSC)	IT	Sheno Poly_technic College	0911835002 0912068479	tedmutd@gmail.com
9	SUBAGADIS GIGAR	B (BSC)	CSIT	MoLS	0920193853	subiartpromo@gmail.com