ICT SYSTEM SUPPORT NOTES

LECTURE ONE & TWO

Unit Code: IT/OS/ICT/CR/4/6

Unit Title: ICT SYSTEM SUPPORT

Department: Information Technology

Year 1 term 3

Lecturer's Name: Geoffrey Mutiso

Email Address: milesjeffn5@gmail.com

LECTURE ONE

What is ICT?

ICT, also known as Information and Communications Technology, is the infrastructure that facilitates the communication of people and organizations in the digital world. Generally, it includes applications, devices, systems, and networking components that enable modern computing.

Information and Communication Technologies (ICT) is used in all spheres of life. It has changed the way everything functions, be it learning, solving problems, or working. The tools of ICT such as communications, networked computers, and media have become crucial for the efficient working of all professions. Today, it is almost impossible to imagine the functioning of organizations without these tools. ICT tools have changed the time and space of learning and working, which has been beneficial for the students as well as the working professionals.

ICT comprises of two parts:

IT [Information technology]: It refers to the use of storing, processing, collecting data. All the different components of the computer, like hardware and software, come under this category.

CT [Communication technology]: It refers to the use of technology for telecommunication, broadcasting media, audiovisual processing and transmitting information, and transmitting information through wired or wireless networks.

- ✓ ICT as a whole is a combination of IT and CT, where we collect, store, process, and transmit data through wired or wireless methods.

What is an ICT system?

An ICT system is an input, process and output. It transforms data into useful information that people can use. The input collects the data, the process transforms the data into useful information and the output delivers the final information.

Qualities and characteristics required of an ICT professional

Some of the skills that are essential to have in an ICT related job includes the following;

1. **Good oral and writing skills**

Writing reports and documents in a suitable style is essential for the job. Documents need to be created to help solve solutions in the future. Workers need to discuss problems and give feedback and they need to be able to speak about things the client will understand.

2. **Good listener**

Need to be a good listener to obtain a clear understanding of what the user requires and meets the needs to produce the end system.

3. **Integrity**

The employee must be trustworthy. An individual might have access to sensitive data and it is important they don't misuse it.

4. **Team worker**

The ability to work effectively in a team. You need to be sensitive to the needs of others, reliable, supportive and co-operative. Ideas are freely shared.

5. **Able to adapt**

Software changes fast, you need to be able to adapt with it. You need to adapt to new working methods and when doing projects, they may overlap or you need to swap between teams, so you need to be able to cope with change.

6. **Attention to detail**

You need to spend time thoroughly checking work to avoid mistakes. For example, people involved in entering data into a live computer system need to work with a high level of accuracy, incorrect data leads to incorrect information.

7. **Creative flair**

In ICT you need to come up with new ideas for jobs and ways to solve problems. You will need to possess a strong visual sense and good spatial awareness as well as sound technical knowledge.

8. **Good problem solver**

To be able to approach problem solving in a systematic and logical way is essential for many ICT roles. Many organizations require new employees to take aptitude tests.

9. **Work under pressure**

The ability to meet deadlines is essential. It is possible that you will have to work long hours to fix a problem that needs to be resolved as soon as possible. Work should not be left to last minute.

10. **Work flexible hours**

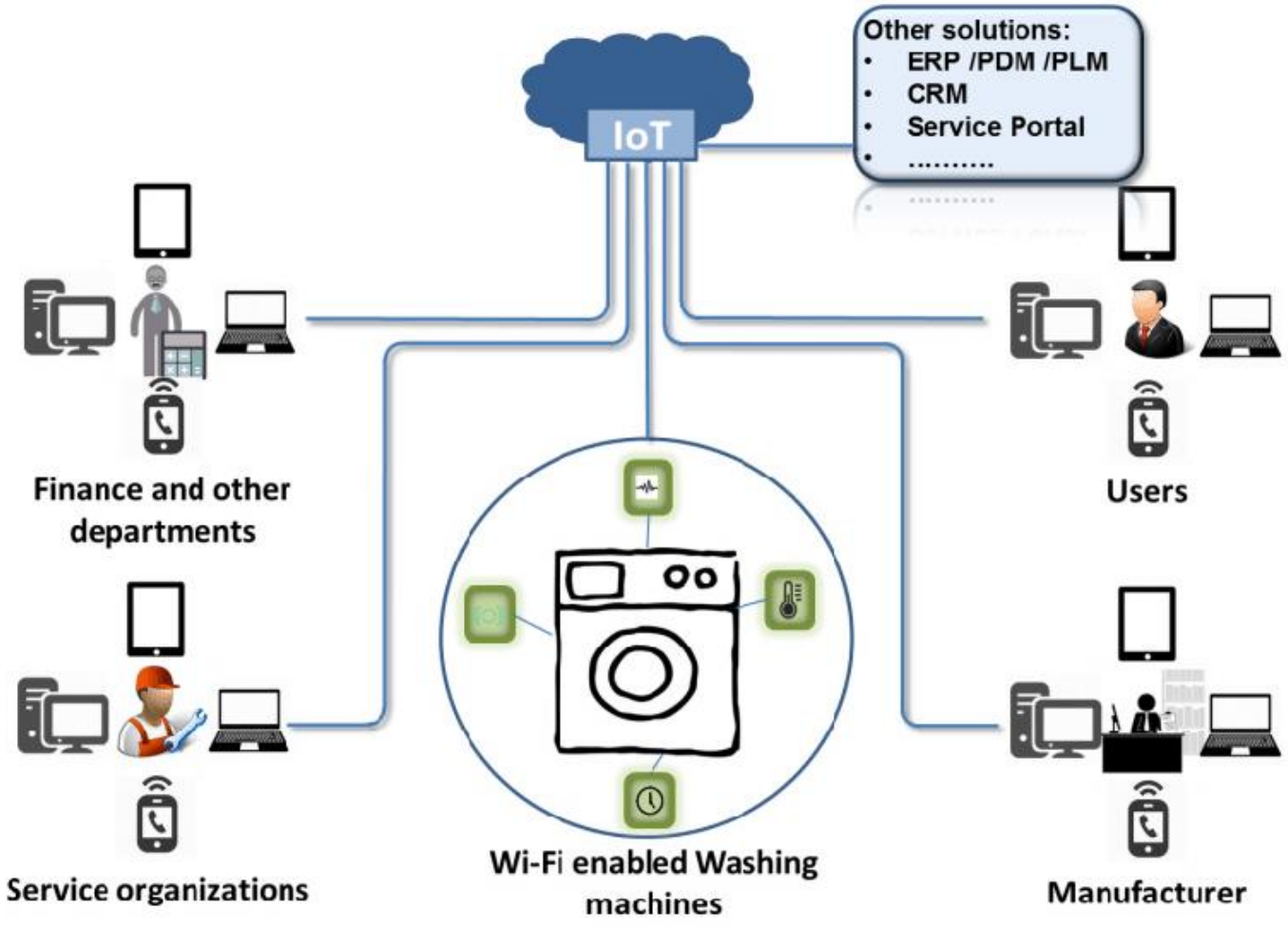
In certain jobs you need to be able to work flexible hours. For example, if you work for a multi-national organization in London but your users are located in America, you need to be able to provide support for them. Sometimes a job will need you to be on call so you will need to be available if a job pops up.

ICT INFRASTRUCTURE

ICT Infrastructure means the information and communications technology infrastructure and systems (including software, hardware, firmware, networks and the Company Websites) that are or have been used in the Business.

Information and Communications Technology (ICT) infrastructure represents equipment and software necessary to implement and operate systems and networks for communications services as well as support applications, digital content, and ecommerce.

ICT INFRASTRUCTURE OVERVIEW



Components of ICT System infrastructure.

The components of ICT allow people to interact with each other in the digital world. A list of components of the ICT system is mentioned below. However, ICT is not limited to the list as it includes any application, system, or device that enables the digital interaction of organizations and people.

There are typically 6 components to an ICT system,

1. **Data**

The word Data is derived from Latin, which means something given. Data is the plural word, and its singular form is Datum. At the initial stage, the data we provide to the computer is raw. Then, the computer processes it and converts it into information. This data can be present in the form of images, documents, audio clips, software programs or any other form. This data is processed

with the help of a CPU and stored in the hard disk of the computer. Computers store the data in the form of binary numbers means in the form of 1 and 0. There are 5 types of data present:

- ✓ ***Text Data***: It contains all the alphabets from A-Z.
- ✓ ***Number data***: It contains numbers from 0-9.
- ✓ ***Alphanumeric Data***: It contains various symbols like @, #, $, %, &, *, and many more.
- ✓ ***Image Data***: It contains images in formats like JPEG, PNG, and JPG.
- ✓ ***Audio-Video Data***: It contains data in different formats like MP3, MP4, and HD..

2. Hardware

The physical components. It is divided into two types:

Internal Hardware

They are found inside the system unit, which includes the motherboard, CPU, RAM, ROM, graphics card, fan, sound card, expansion slot, and different types of drives.

External Hardware

It is the physical part of the computer like the monitor, keyboard, or mouse. External hardware components are input devices, output devices and storage devices; these are known as peripherals. It is further divided into -

- ✓ ***Input Devices:*** These are used to ender data in the computer, e.g., keyboard, scanner, joystick, light pen, etc.
- ✓ ***Output devices:*** They receive the information from the computer and convert it to a readable format. e.g., monitor, speakers, printer, headphone, etc.
- ✓ ***Storage Devices:*** These are used to store data. E.g., the optical disk, floppy disk, USB flash drive, memory card, etc.

3. Software

Software is a set of programs or instructions which tell a computer how to work. The software executes tasks, which are specific in nature, through the set of instructions that operates them. Software is digital portions that run with the help of hardware. Software is of two types:

Application Software:

These are downloaded by the user according to needs, such as games, antivirus, browsers, and many others.

System Software:

These include operating software like Mac OS or Windows. System software runs without user intervention.

4. **Information**

Refers to the data that is converted to give it a meaning. Information system infrastructure refers to the range of devices and technologies, applications and systems, standards and conventions that the individual user or the collective rely on to work on different organizational tasks and processes.

5. **Procedures**

Refers to the series of actions conducted in a certain order to make sure the system runs smoothly.

6. **People**

Data is entered by humans, for example a keyboard. Without competent , well qualified people in charge of running and maintaining your infrastructure, you will artificially limit the capabilities of your organization.

In large organizations, you will find specialty positions for each ICT area. In small organizations, you will find that the general systems administrator handles many of the roles.

To remember the components, use this sentence

People Hate Slimy Dogs In Poland

(People, Hardware, Software, Data, Information, Procedures)

TYPES OF ICT INFRASTRUCTURE

1. **Computer hardware platform**

These are computers and server machines in your organization. Servers allows users to share information and the necessary files required to keep the company running.

Machine hardware is made up of the following;

The processor or the system with high performance, several processors. Some processors allow limited programmability like most video accelerators while in the others, you can program them fully.

- ✓ Software development environment.
- ✓ Bus interface

- ✓ I/O devices that are provided by the platform.

Some manufactures of computer hardware and servers include IBM, Apple, Hp, DELL, among others.

2. Enterprise and software Application

Enterprise application is a large-scale software that helps solve the problems of the entire organization. They include software such as middleware, oracle, and Peoplesoft. Other applications in the companies used to link all the other applications also fall into this category. They offer computer-based, essential business tools such as;

- ✓ Email marketing system
- ✓ Automatic billing system
- ✓ Human resource management
- ✓ Business intelligence
- ✓ Online payment processing
- ✓ Internet service management

3. Operating system platform

An operating system is a software that manages the functioning of all the other applications after being loaded on a computer. It also acts as the interface for the user. Every computer must have at least one operating system for it to function.

OS such as Windows, macOS, and servers like Linux are used by the employees and other personnel in the company for communication, storage, and access of data.

4. Data storage and management

Data management is handled by software and stores in storage devices. Nowadays has evolved as a need to access it easily, backing up and restoring data grows. There are two types of storages;

- ✓ *Traditional storage*- in this type of storage, data is stored in computers or servers and you can access it through LAN/WAN. Information is stored on disks that are easy to reformat when needed. The number of disks is added as information increases. Additionally, data is stored in different locations to avoid total loss in case of break down or disaster.
- ✓ *Cloud storage*- in this type of storage, data is stored in third party servers on the cloud. It can be accessed any time from anywhere by even multiple users at the same time. However, in case the system is down and the backup provided as failed, there is no other way to access it. Additionally, it is more insecure compared to traditional storage.

5. **Networking and telecommunication platforms.**

Networking platforms includes windows server OS, Linux, Unix, among others. telecommunication platforms are provided by telecommunication companies that provide data connectivity, internet access, voice, and wired area network. Leading companies in this industry include Telstra and others. However, other companies are raising rapidly offering WI-FI, cellular wireless, and internet services. In the company, these infrastructures include telephones, cables, mobile technology such as 5G, and networking infrastructure like networking hardware, software, facilities, and services.

6. **Internet platforms**

This relates to and sometimes overlap with network infrastructure and hardware and software platforms. In company, infrastructure related to the internet include hardware, software, and facilities that support web hosting, maintenance of websites, web application tools together with intranets and extranets. Companies that offer web hosting services usually maintain large servers or several servers and also offer their subscribers to a space to hoist their websites at a fee.

7. **Consulting and integrated services**

These are used to integrate the legacy system with modern infrastructure. Software integrating is ensuring that new technology works with the old one. Also called legacy system.

Companies continue using their old system since replacing them is very expensive. If they can work perfectly with the new infrastructure then there is no need to replace them. They hire consulting and integrated services so that they can find the best way to match the two infrastructures according to their business process.

The business of consulting and system integration is lucrative for enterprise software companies like IBM who, apart from providing hardware, also offer the service.

How does these ICT Infrastructures Work Together?

Without any of the components above, the IT infrastructure is not complete and cannot work as expected. The most basic and obvious is hardware. A company requires computers, routers, switches, among others to function.

Without software, the hardware is useless. You'll need applications and software like Enterprise Resource Planning (ERP) and Business Intelligence (BI) among others. Some are bought from providers while others can be developed by the IT department depending on your business needs.

Additionally, the internet is an essential part of conducting business in this age. Your employees will depend on network connectivity to send and receive emails, web access and even keep the corporate website running. Routers, switches, networking hubs, and computers have to be connected inside of a network.

Also, your business data will be stored in hardware like servers or more modern methods where you can access it through a network.

However, all of this is not possible without operating systems that function as a user interface.

Conclusion

All the components of IT infrastructure depend on each other to keep your business running. The software cannot function without hardware which is also almost useless without a network and internet connection. Also important are the people who operate these infrastructures to keep them working.

ICT INFRASTRUCTURE DOCUMENTATION

Why is ICT infrastructure documentation important?

Preparing and maintaining documentation for your IT infrastructure isn't a glamorous part of keeping your IT systems running smoothly. Further, it's not something you'll use every day. However, it is a critical tool if something goes wrong.

And as hard as you try, something will go wrong.

Assume you experience a catastrophic network failure. How will you provide backup if you don't have your infrastructure documented? What would happen if you had a network problem that you needed to troubleshoot? A support professional will need to review the infrastructure in order to troubleshoot the problem and locate a specific failure. And, these are just a couple of examples of when you need infrastructure documentation.

Lack of documentation is a leading cause of costly and time-consuming troubleshooting.

When an IT support professional must start from scratch to find IP addresses, physical locations, dependencies and passwords, the time to fix a problem will naturally be much longer and more costly than if documentation were available.

In addition, infrastructures change. Some network experts find that a new network diagram stops being up to date around the time they're printing it. To combat this phenomenon, it's important that you document and update the documentation on a regular basis.

The steps you need to take

These steps will help you save time and money, keep your technology running well, and let you spend your time running your business.

1. **Develop a policy**

A policy will ensure that everyone involved understands the goal of maintaining accurate documentation. Include a description of the components of the infrastructure that need to be tracked, and the role each responsible administrator will play in keeping the documentation updated.

2. **Create a diagram**

A visual description will illustrate an overview of the infrastructure. Some diagrams can include everything in one place, including the network segments, routers, servers, and gateways. For larger organizations, you may need to create an overview, and then develop separate maps that go into the detail required for specific areas.

3. **Maintain change logs**

Often a failure in a server or other component relates directly to a change. When you maintain a log of things such as software versions and patch and application installs, you can use it for troubleshooting and to provide a roadmap if you experience a catastrophic failure.

4. **Describe all hardware components**

All hardware needs to be documented, not just servers. Information to document includes how each device is configured and connected to the network, as well as passwords or password hints.

5. **Affix labels to all hardware components**

It’s very possible that outside IT support professionals will assist your IT staff, especially when problems occur. Your documentation will only be effective if anyone involved can match the components on your diagrams to your physical hardware.

Assignment:

How does infrastructure documentation benefit your business?

LECTURE TWO

TOOLS FOR ICT INFRASTRUCTURAL SUPPORT

Classification of ICT tool, device, infrastructure	ICT tools used
Web based tools and Applications for managing learning and teaching	Learning management systems, Student management systems, Digital student report card systems, Plagiarism detection systems, Online Collaborative workspaces, Virtual classroom software systems and e-Portfolios
Learning and Teaching tools	Interactive whiteboards, Digital communication,
Mobile delivery devices	Storage devices, Personal Digital Entertainment devices and MP3 players, Personal digital assistants, Mobile phones, Laptops, Tablet PCs, Gaming devices, Assistive and Adaptive technologies
Content delivery methods	Podcasts, Vodcasts, Blogs, Wikis, VoIP, Digital TV,
Other devices, concepts and technologies	Moblogs and photologs, Digital cameras, Scanners, Swarming, Peer-to-peer networking and technologies

ICT Infrastructure auditing

If things are not looking up in the IT department lately, or there have been a lot of downtimes, then it's time for an IT audit!

We will discuss about;

- ✓ What is an IT audit
- ✓ Importance of an IT audit
- ✓ Components of an IT audit
- ✓ How to prepare for an IT audit
- ✓ IT audit process

What is an IT Audit?

IT audit, also known as, information system audit is the examination of an organization's IT infrastructure, policies, and procedures.

IT audits started in the mid-1960s and have gone through several changes. They play an important part in keeping an organization's IT policies and procedures up-to-date.

Importance of An IT Audit

Every business needs an IT department. It may be an internal team, remote team, or maybe you outsource your organization's IT tasks.

In any case, the threat of cyber-sabotage is real. A cybercriminal can steal your data, and ruin your enterprise's reputation leading to a major loss.

In the information age, data is your biggest asset. Unlike physical assets, you cannot protect data by building walls and safes. Cyber threats are like Trojan horses, appearing friendly, but holding surprises.

However, the threat does not necessarily come from outside. It can also be internal. Like an employee misusing or mishandling IT equipment. For example, a phishing attack can happen if an employee clicks on an insecure link on their work computers.

In conclusion: technology is vital AND vulnerable!

What your business needs, is someone to analyze the complete IT infrastructure and make sure that your assets are safe. Remember, the integrity of your IT system can be the difference between success and failure!

Components of an IT Audit

IT audit can be broadly divided into two types:

IT General Controls (ITGC): they exist to assure the integrity, availability, and confidentiality of data. These are the basic controls applied to IT systems including applications, operating systems, databases, and support.

IT Application Control (ITAC): it's a security measure put in place to restrict unauthorized applications from putting the system and data at risk. The ITAC includes identification, authorization, authentication, input controls, etc.

More specifically, the five categories of IT audit are:

- **System and Application**: this audit focuses on the system and application in an organization. It verifies that the system and all applications are efficient, appropriate, reliable, up-to-date, and secure on all levels.
- **Information Processing Facilities:** It verifies that all processes are working efficiently, accurately, and timely, in both normal, and rather disruptive conditions.
- **System Development:** this audit verifies that the under-development system is aligned with the organization's objectives. It also makes that the system is made per the generally accepted standards for systems development.
- **Management of IT and Enterprise Architecture:** it ensures that IT management is structured and the information processing environment is efficient and controlled.
- **Client/server, Telecommunication, Intranet, and Extranet:** this audit focuses on telecommunication controls. It ensures that proper measures are in place for the server, client, and network connecting the server and the client.

Purpose of IT Audit

The purpose of an IT audit is to evaluate the effectiveness of an organization's IT system.

Installing controls keeps everything in check, but is not enough in the long-term. It's important to make sure that the proper controls are installed and working as intended. If it's not, then how can we handle the situation and prevent future breaches.

With the way technology is advancing, we also need to consider its impact on information security. It's important to check if the controls put in place a few years ago, is still efficient and enough.

In an IT audit, all these questions are answered by an unbiased and independent entity. The auditors are auditing the information system. In an information systems environment, the audit is the evaluation of the information system, inputs, processing, and output.

An IT audit evaluates three major aspects of an information system:

- **Availability**: will the information system be available when the users need it?
- **Integrity**: will the information system be reliable, accurate, and prompt?
- **Confidentiality:** will the information in the system be restricted to authorized parties?

How to Prepare for an IT Audit?

In organizations, people often ask how to prepare for an IT audit. If there is anything we can do to make the process go smoothly.

If you have an upcoming Audit and want to prepare for it, then here are a few steps to ensure a stress-free IT audit.

Notify All Internal and External Partners

The first step in an IT audit is to notify the external and internal partners that an audit is coming. It includes all the stakeholders, management, and support. The whole team should be ready to provide any documentation or details that the auditors request.

You should notify all departments and ensure that everyone's ready to make the process go smoothly.

A great way to make the audit process go smoothly is to make a list of all IT individuals and management who can be relied on to deliver.

You can also conduct surveys to ask the staff about any IT-related issues and their severity.

Step 1: Create an IT Asset Inventory

An IT audit is all about IT assets and securing them. Creating an Inventory of all IT assets in your organization can put everything into perspective. The IT assets include both hardware and software resources that are used in everyday operations.

Along with IT assets inventory, you should also keep the access linked list handy. It should be easier for auditors to have immediate access to your system.

To make this work, create a list of login credentials for all software and hardware resources involved in the audit process. Also, in terms of physical access in the building, auditors should be able to freely visit various parts of the property.

Step 2: Ask Your Auditor for a Document Checklist

During the IT audit, the auditors will request various documents at different stages. keeping a list of all important documents in your organization will come in handy.

Ask your auditors to provide a list of all documents that they may need and get your documentation right. Having all important documents in a central location can save both you and your auditor a lot of time and trouble.

The documentation entails all contracts with third-party service providers and external vendors. The list should also include purchase and warranty documents of your IT infrastructure. Knowing how old your equipment is crucial in several ways.

You should also have a log of the administrative written policies and procedures in one place.

Step 3: Prepare Your Financial Statements

A primary reason why most organizations conduct an IT audit is to reduce the operational cost of their IT infrastructure. To reduce costs, you must create a financial statement covering all expenditures related to the IT setup.

When the auditors have a complete picture of your finances and expenditures, they can make suggestions about reducing operating costs and increase profit.

Step 4: IT Policies and Procedures

Before conducting an IT audit, you need well-documented IT policies and procedures. A softcopy and hardcopy of the policies and procedures ready for the auditors to review. This will save you time and trouble that would otherwise be spent scrambling through the policies and procedures looking for something specific.

On the other hand, the auditors will save time otherwise spent asking for various documents at various stages.

Step 5: Ensure a Written Information Security Plan

Next to the IT policies and procedures, you should also have a written information security plan in place.

All firms that are registered with the Security Exchange Commission (SEC) are required to have a written information security plan. A written ISP (Information Security Plan) can help prepare the organization for IT-related risks and measures to handle it.

Regarding an information security plan, a lot of organizations have no idea where to start. this leads to unnecessary and time-consuming work. Automated tools and processes should be used to make the process effortless. You can also hire an expert auditor to help you through the process.

Step 6: Create a List of Controls and Safeguards

Whether big or small, in an IT infrastructure, controls and safeguards are one of the most important aspects. You must have proper controls at strategic points to keep the applications and software secure. And create a list of all controls and save that you have in place for the IT system

Step 7: Conduct a Gap Assessment

Being aware of the gaps in your IT infrastructure can make the IT audit go more smoothly. You should also have a grasp on apps and services to better understand and secure them.

No system is entirely fool-proof, and as a user, you're best-equipped to find vulnerabilities in your system.

Step 8: Perform a Self-assessment

Auditors are definitely the best for an audit but no one knows the system better than you. A self-assessment of your system will help you get a better understanding of your organization.

A self-assessment will also give you confidence about your system's performance and help you understand the audit results better

Step 9: Findings from Previous Audits

If this is your first IT audit, then you can skip this step. However, if it's not, then make sure to present the auditors with the findings from the previous audit.

Any issues found in the previous audits that were not addressed before should also be mentioned.

Step 10: Schedule Tests or Deliverables

Starting an IT audit with all your test and deliverables scheduled for after the audit can show in a negative light. Perform some basic tests and have deliverables beforehand

Step 11: Be Prepared for Anything

After the audit may not like the findings. Be prepared for anything. Going into the audit with the proper mindset can help prepare you for any kind of results

Step 12: Get A Second Opinion

Getting a second opinion about the findings of the auditor is not a bad thing. It gives you a head start when you get the results. It also helps you prioritize the results and begin the remediation process.

IT Audit Process

An IT audit guide is not complete without the audit process, which includes five steps.

1. Planning the IT audit
2. Studying and evaluating controls
3. Testing and assessing controls
4. Reporting and documenting the results
5. Follow-up

What will be the ICT deliverables?

An ICT audit deliverable includes the following documentation;

- ✓ Planning of the audit scope and deliverables
- ✓ Description of the criteria
- ✓ Audit program.
- ✓ Audit steps and evidence.
- ✓ Contribution of other auditors and experts
- ✓ The final audit findings, conclusions, and recommendations.
- ✓ Audit documentation
- ✓ Audit work to put
- ✓ Evidence of audit supervisory review.

The audit report should include the following;

- ✓ Introduction (Executive summary)
- ✓ Finding and results
- ✓ Conclusion
- ✓ Any reservation (with regards to audit)
- ✓ recommendations

TROUBLESHOOTING.

Is the process of diagnosing the source of a problem. It is used to fix problems with hardware, software, and many other products.

Steps in troubleshooting

i. Identify problem.
ii. Establish a theory of probable cause
iii. Test the theory to determine the cause
iv. Establish a plan of action to resolve the problem and implement the solution
v. Verify full system functionality and if applicable, implement preventive measures.

Basic Troubleshooting techniques

ICT infrastructure safety and precautious measures

Following are 10 safety tips to help you guard against high-tech failure:

1. **Protect with passwords.**

This may seem like a no-brainer, but many cyber-attacks succeed precisely because of weak password protocols. Access to all equipment, wireless networks and sensitive data should be guarded with unique user names and passwords keyed to specific individuals. The strongest passwords contain numbers, letters and symbols, and aren't based on commonplace words, standard dictionary terms or easy-to-guess dates such as birthdays. Each user should further have a unique password wherever it appears on a device or network. If you create a master document containing all user passcodes, be sure to encrypt it with its own passcode and store it in a secure place.

2. **Design safe systems.**

Reduce exposure to hackers and thieves by limiting access to your technology infrastructure. Minimize points of failure by eliminating unnecessary access to hardware and software, and restricting individual users' and systems' privileges only to needed equipment and programs. Whenever possible, minimize the scope of potential damage to your networks by using a unique set of email addresses, logins, servers and domain names for each user, work group or department as well.

3. **Conduct screening and background checks**.

While rogue hackers get most of the press, the majority of unauthorized intrusions occur from inside network firewalls. Screen all prospective employees from the mailroom to the executive suite. Beyond simply calling references, be certain to research their credibility as well. An initial trial period, during which access to sensitive data is either prohibited or limited, is also recommended. And it wouldn't hurt to monitor new employees for suspicious network activity.

4. **Provide basic training.**

Countless security breaches occur as a result of human error or carelessness. You can help build a corporate culture that emphasizes computer security through training programs that warn of the risks of sloppy password practices and the careless use of networks, programs and devices. All security measures, from basic document-disposal procedures to protocols for handling lost passwords, should be second-nature to members of your organization.

5. **Avoid unknown email attachments.**

Never, ever click on unsolicited email attachments, which can contain viruses, Trojan programs or computer worms. Before opening them, always contact the sender to confirm message contents. If you're unfamiliar with the source, it's always best to err on the side of caution by deleting the message, then potentially blocking the sender's account and warning others to do the same.

6. **Hang up and call back**.

So-called "social engineers," or cons with a gift for gab, often prey on unsuspecting victims by pretending to be someone they're not. If a purported representative from the bank or strategic partner seeking sensitive data calls, always end the call and hang up. Then dial your direct contact at that organization, or one of its public numbers to confirm the call was legitimate. Never try to verify suspicious calls with a number provided by the caller.

7. **Think before clicking.**

Phishing scams operate by sending innocent-looking emails from apparently trusted sources asking for usernames, passwords or personal information. Some scam artists even create fake Web sites that encourage potential victims from inputting the data themselves. Always go directly to a company's known Internet address or pick up the phone before providing such info or clicking on suspicious links.

8. **Use a virus scanner, and keep all software up-to-date.**

Whether working at home or on an office network, it pays to install basic virus scanning capability on your PC. Many network providers now offer such applications for free. Keeping software of all types up to date is also imperative, including scheduling regular downloads of security updates, which help guard against new viruses and variations of old threats.

9. **Keep sensitive data out of the cloud**.

Cloud computing offers businesses many benefits and cost savings. But such services also could pose additional threats as data are housed on remote servers operated by third parties who may have their own security issues. With many cloud-based services still in their infancy, it's prudent to keep your most confidential data on your own networks.

10. **Stay paranoid**.

Shred everything, including documents with corporate names, addresses and other information, including the logos of vendors and banks you deal with. Never leave sensitive reports out on your desk or otherwise accessible for any sustained period of time, let alone overnight. Change passwords regularly and often, especially if you've shared them with an associate. It may seem obsessive, but a healthy dose of paranoia could prevent a major data breach.

Protecting your data does not guarantee enough safety. We should also consider health and safety measures in our working environment. Don't forget that rules for all electrical appliances apply in a computer room. This means:

- ✓ There should be no trailing wires
- ✓ Food and drink should not be placed near a machine
- ✓ Electrical sockets must not be overloaded
- ✓ There must be adequate space around the machine
- ✓ Heating and ventilation must be suitable
- ✓ Lighting must be suitable with no glare or reflections
- ✓ Benches and desks must be strong enough to support the computers

When installing/removing computer hardware and other peripherals:

- ✓ Wear proper apparel. Avoid acrylic or wool sweaters when working with electronic parts. Do not wear loose fitting clothing, rings, bracelets etc.
- ✓ Unplug all computer equipment and peripherals before opening any covering cases.
- ✓ Keep your work area clean and well lit.
- ✓ Check for damaged parts.
- ✓ Do not force components into computer ports.
- ✓ Use an anti-static wrist strap or discharge yourself by touching a grounded metal object such as a computer casing.
- ✓ Power supplies produce several levels of voltage. Read the information on the power supply carefully and make sure that the power supply you are using is appropriate for the application.
- ✓ Replace all cases or coverings after inspections or installations.
- ✓ Check all circuits and installations with the instructor before power is applied.
- ✓ Retain all screws during disassembly in containers such as film canisters for proper re-assembly.
- ✓ Electronic components should never become hot. Hot components means that there is a problem with the circuit. Disconnect any power immediately.
- ✓ The most important safety rule of all: Always Be Careful! (ABC)

ICT Prevention measures

Causes of hardware and software failure

Causes of software failure

Most software projects fail completely or partially because they don't meet all their requirements. These requirements can be the cost, schedule, quality, or requirements objectives. According to many studies, the failure rate of software projects ranges between 50% – 80%.

Common Software Failure Causes

There are a variety of causes for software failures but the most common are:

1. Lack of user participation
2. Changing requirements
3. Unrealistic or unarticulated project goals
4. Inaccurate estimates of needed resources
5. Badly defined system requirements
6. Poor reporting of the project's status
7. Lack of resources
8. Unmanaged risks
9. Poor communication among customers, developers, and users
10. Use of immature technology
11. Inability to handle the project's complexity
12. Sloppy development practices
13. Poor Project Management
14. Stakeholder politics
15. Lack of Stakeholder involvement
16. Commercial pressures

Causes of computer hardware failure

1. Extremes of environments
2. Temperature
3. Humidity
4. Ingress of dusts or liquids
5. Shock
6. Vibration
7. Signal screening
8. Cable separation
9. Power conditioning
10. Site-specific environment

So how do you overcome these failures?

When we look at computer hardware solutions fit for industrial applications, there are a many possible solutions available, but they can be broadly categorized as :

1. **Re-engineering commercial hardware**

Often, many of the problems above arise from commercial computer hardware typically designed for benign rather than challenging environments.

Where possible, replace commercial components with appropriate industrial-grade equivalents. Where some hardware must remain commercial computer consider if this can be re-engineered or re-packaged for industrial applications, without reducing operational life, reliability or product warranty.

For large scale programmes, we would typically revise the equipment design or repackage solutions to deliver optimized volume manufacture.

This will provide a balance of high-speed build times with minimized modification costs, and as the overall volume increases, will secure a more cost-effective solution when compared to modifying existing equipment on a case by case basis.

2. **Partnering with the right vendors**

The second approach is best used where the number of implementations is low but the volume of equipment installed is high.

For this scenario, working with a partner to define a bespoke solution that uses components from multiple vendors, where components can be selected to best suit the potential problems it may encounter as it is specified.

This approach will unlock the best from each element and bring them together into a product that secures the advantages of commercial performance while being suitably protected to endure the challenges of its environment.

3. **Changing your environment**

It seems obvious, but preventing the problem, rather than protecting against it, can be a valid approach. This can be a fundamental change in the environment through the use of a protected building, shelter or room, or a change in application scope and architecture that places the equipment into a less hostile environment. Of course, this isn't always a viable approach for lots of reasons, and where the right computing solution to mitigate the issues is crucial.

Causes of Failure in Operating System

A system failure can occur as a result of a hardware failure or a serious software problem, causing the system to freeze, reboot, or entirely stop working. A system failure may or may not result in an error being displayed on the screen. Without warning or error message, the computer may shut down. On Windows computers, an error message is frequently displayed as a Blue Screen of Death error.

The failure of the operating system might be caused by one of two things. The following are the reasons:

- ✓ Hardware Problems
- ✓ Software Problems

Hardware Problems

The failure of the operating system can be caused by a variety of hardware issues. The following are some examples of hardware issues:

1. **Overheating:**

The most common cause of operating system failure is overheating. It's simple to rule out overheating. To keep a computer's CPU cool, it has a fan built-in. The fan may get old and ineffective over time, or it may just be unable to keep up with the demands of your computer.

2. **Power Problem:**

Incorrect functioning of the System Power Supply can result in the System being shut down instantly.

3. **RAM:**

Because the OS is unable to access data stored on the RAM chip, a damaged RAM chip may cause system failures.

4. **Bad Processor:**

A defective processor can and often does result in system failure, as the system may not function properly if the CPU is not working properly.

5. **Motherboard Failure:**

Because the computer is unable to execute requests or function in general, a failing motherboard may result in a system failure.

Software Problems

The failure of the operating system can be caused by a variety of software issues. The following are some examples of softwarxbje issues:

1. **Thrashing:**

When two programs compete for control of the same resource, a deadlock occurs. During a stalemate, the operating system may attempt to switch between the two programs. It eventually leads to thrashing, which causes a system crash by overworking the hard disc by transferring information between system memory and virtual memory.

2. **Corrupt Registry:**

The registry is a small database that contains information on the kernel, drivers, and programs. Before starting any app, the OS searches its registry. Erroneous application uninstallation, thoughtless registry updates, or having too many installed applications, among other factors, can cause registry corruption.

3. **Improper Drivers**:

To use additional hardware, you'll need drivers, which may usually be acquired from the internet. Bugs could be present in these drivers. The operating system crashes as a result of these defects. The "Safe Mode Boot" option is available in most recent operating systems. Safe Mode Boot is used to locate and resolve malfunctioning drivers. In Safe Mode Boot, just the most important drivers are installed, not all of them.

4. **Virus:**

A virus can replicate itself on a computer system. Viruses are particularly harmful since they can alter and erase user files as well as damage computers. A virus is a little piece of software that is embedded in the operating system. As the user interacts with the program, the virus becomes embedded in other files and programs, potentially rendering the system unusable.

5. **Slow System Performance:**

The system's performance has deteriorated significantly. It's the ideal sign if you're seeking how to spot signs of operating system failure on the internet. In this instance, check to see if you have the most recent versions of Windows installed on the PC. Even security patches must be updated on a regular basis. The system will then restart normal operation.

6. **Compatibility Error:**

When the old apps in Windows stop working after an upgrade, this type of problem is widespread. You are aware that this is one of the operating system breakdown symptoms when you face it, but you can quickly resolve it. In most cases, Windows has a feature that allows apps to be updated to work with the latest version. You can run the software in compatibility mode if you are a computer specialist and are familiar with the language.

7. **Failure to Boot:**

The OS may have been damaged if you are unable to boot. The boot order of the system has been altered. The booting process and sequence setup can be examined. You must reinstall Windows if the operating system fails. Please keep in mind that the issue could be serious. It's one of the most reliable symptoms of a failing operating system.

8. **Trojan Horse:**

The user's login information is saved by the application. Trojan Horse prohibits the transfer of user information to a rogue user, who can then login and access system resources.