COURSE CODE:	ITP111
COURSE DESCRIPTION:	System Administration and Maintenance
COURSE INTENDED LEARNING OUTCOMES:	1. To have a working knowledge of the critical concepts of system administration 2. To develop documentation and audit of select systems administration & maintenance concerns 3. To resolve system administration and maintenance issues and challenges
LEARNING MATERIAL FOR WEEK NUMBER:	3
I. TITLE:	Performing System Audits and Documentation
II. OBJECTIVES:	After this lesson, you are expected to be able to: 1. explain what *System Administration and Maintenance* is all about 2. successfully identify critical operating system commands and operations 3. perform simple system administration check-up and audit
III. INTRODUCTION:	This module is about the audit and documentation portion of the *Systems Administration and Maintenance*. The students will be led through the processes of system audits to ensure that systems are functioning in accordance with set criteria. Another overlooked process is the system documentation which provides admins and maintenance staff the guide through the system without having to too much guesses from previous activities within the system. For laboratory activity, this lesson also provides the steps through the audit and documentation processes. Future system trouble shooting and re-configuration are also likely helped by system audits and documentation.
IV. CONTENTS:	

Lesson Coverage:

1. What is s*ystems audit*?
2. Importance of system documentation

What is Systems Audit?

If there is one very plausible functionality systems have to offer, it is the audit processes. Computer systems are quite easy to deal with since they produce a lot of audit trails. A system audit may be undertaken by system admins, but independent bodies (either internal or external to the organization) should take the charge to allay fears of system manipulations and fraudulent behaviors.

Generally, there are **three types of audits**:

1. Process audit - intended to evaluate and audit the processes to ensure they are working as intended
2. Product audit - evaluation of a specific product or a service against the required specifications or performance standards
3. System audit - an audit on a system (most likely involving computing systems) to validate whether or not the elements of the system are effective and properly implemented to meet the objectives or standards

A system audit is supposed to be an independent and systematic examination of the management controls within an information technology infrastructure. This is quite a user-centric approach to system audits.

Another way of describing system audit is the verification of a company's IT engagements, activities and the verification of the results needed to achieve the intended results. This is approach is a broader one with the end view of seeing whether the systems are able to deliver desired results.

On the other hand, the ISO (under the ISO 19011:2018) defines an audit as:

> …the "systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the audit criteria are fulfilled."

The above ISO definition provides another way of looking at a system audit as the process which independently examines the proper functioning of systems against defined audit criteria.

Audits are abhorred in many respects since they demand accountability, checks, inspections, documentations and other related activities which most of the times results to findings which are not amusing. Not to be unappreciated, a system audit is important as it allows an organization to review the performance of its operational systems.

By performing a system audit, companies can:

1. Evaluate the **actual performance** of their operations compared to what was **planned**
2. **Validate that the objectives** pursued by the organization remain relevant
3. Validate whether or not the company is **achieving those objectives**
4. Ensure that the systems used are **reliable**
5. Review system records to ensure systems **operate based on specifications**
6. Identify **vulnerabilities** and **risks**
7. Allow a company to define a **mitigation plan** to better achieve its objectives
8. Monitor its **operational systems** to ensure they meet the objectives on an ongoing basis

Scope of a system audit

The scope of a system audit can be considered as the normal achievement of the results expected depending on the objectives.

1. Accuracy

   For instance, if the scope of the audit is to evaluate the correct calculation of a system, then the audit objective will be to assess if the calculations produce the **normal and expected results**.

   Any deviation from what's normal will result in an audit finding.

2. Data Security

   Another example is an audit focusing on whether the systems are compromised. Criteria for audit includes data privacy and data protection.

The scope of that audit should be how the company's systems provide for access restriction, database management, the confidentiality of systems, encryption process and so on.

The normal achievement of the objective is for personal data to be safe and secure.
Any deviations from what's normally expected will result in an audit finding.

Types of system audit

1. Adequacy audit - evaluates a system and assess whether it meets the system requirements and specifications.

2. Compliance audit - evaluates how a system is implemented within an organization to comply with certain standards.
3. Internal audit - carried out by the internal stakeholders within an organization to validate whether or not its systems are properly functioning, effective and achieving their objective; can be performed for any objective important for an organization based on its needs and realities. This type of audit is referred to as a first-party audit
4. External audit - carried out by an outside and independent organization. The external audit is also called the second-party audit. The audit standards can be statutory, regulatory or industry standards, for instance.
5. Extrinsic audit - carried out by an accredited third party. The extrinsic audit is also called the third-party audit.
6. Process audit - an audit of company processes as a whole in light of the objectives being pursued.

The system audit process/phases

1. Audit initiation
2. Audit preparation
3. Audit execution
4. Audit report
5. Audit closure and follow-up

Audit initiation

Audit initiation is the start of the system audit process. During the audit initiation, the auditor and the client will determine the scope and frequency of the audit. When deciding on the scope, importance is given to the client's needs, requirements, objectives and timeline. A client may want to audit the processes in a specific department to achieve the desired objective.

The frequency of the audit can depend on either the client's needs but also any regulatory requirements. If a company is required to perform a systems audit on a yearly basis, that frequency is expected to be met every year. The client can choose to do audits at more regular intervals, which will then depend on the client's needs.

Audit preparation

The audit preparation is when the auditor starts the review of the auditing procedure of the system.
In the preparation phase, the goal is to define an audit plan that typically includes:

1. **Scope** of the audit
2. **Individuals** involved in the audit process
3. System **standards**
4. **Logistics** of the audit
5. **Duration** of the audit process
6. **Meeting** schedules
7. Expected **completion date**

Audit execution

The audit execution is the actual process of performing the system audit. During the audit execution process, the auditor will look at the specifics of the company systems, how they operate, identify what is compliant and what may not be compliant, get clarification from the client and so on. The audit should cover the entire scope of what was agreed upon. Any nonconformity must be identified in an independent and objective way.

Audit report

The final phase of the system audit process is the issuance of the audit report.
The auditor's responsibility is to ensure a report is produced providing an independent evaluation of the audited systems.

The report should be factual and present any discrepancies found along with objective evidence to that effect. The auditor will also provide his or her judgment as to the company's compliance with the system standards against which the audit was conducted.

Audit closure and follow-up

According to ISO 19011, an audit is closed when:
"The audit is completed when all the planned audit activities have been carried out, or otherwise agreed with the audit client." Once all the audit activities have been carried out, the audit process has reached its end.

How to conduct a system audit

Most often, system audits are carried out by IT professionals who are familiar with various information systems and can understand how they are interrelated. Conducting a system audit requires that organizations audit their system hardware, software, data, material and applications.

A system audit is conducted in the following way:

1. **System** review
2. **Vulnerability** assessment
3. **Threat** identification
4. **Internal controls**
5. **Testing**

System review
The first step is a systems review. In this step, the goal is to understand the **IT infrastructure**, the different layers, the management practices and system integration.

Vulnerability assessment
Next is the verification of each application used by the organization and identify which ones are the most vulnerable.
A company cannot eliminate 100% of its vulnerabilities. However, if the vulnerable systems are systematically identified and appropriate controls are implemented, a company can ensure it remains in conformity with the intended standards.

Threat identification
The next step is to define the possible threats to the organization.
Companies face the threat of external actors such as hackers, cybercriminals and external threats. The external actors can also include a company's vendors, suppliers and service providers. They also face internal threats from their own users, programmers, system analysts and so on.

Internal controls
In evaluating the internal controls, a company is evaluating the effectiveness of its internal controls against the standards or threats. If the internal controls do not work as they are intended, the company will need to implement the proper checks and balances to ensure it achieves its objectives.

Testing
The final step is to test and evaluate the various elements of the management system to ensure they meet their objectives and comply with the standards. Different tests can be carried to identify systems that do not work as intended or produce the needed results.

System audit report
The system audit report represents the auditor's faithful assessment of the company's systems and whether or not the systems work as intended in light of the standards or defined objectives.

Audit fieldwork
An *audit fieldwork* is the process where the auditor identifies the processes, systems and technologies expected based on the defined control activities. An auditor's job is to consider the standards or audit objectives and identify the systems and processes implemented by the company to achieve the needed results.

Compensating controls
In some cases, the auditors will find the specific processes or technologies needed to achieve the control objective. In some other cases, they do not find what they are looking to find. If that happens, a company can point the auditor to other controls or other systems that they use to achieve the same result. This is referred to as *compensating controls*. A compensating control is a new system or process found by the auditor that compensates for the absence of the controls they were originally looking to find.

Audit findings
If the auditor looking for a system control objective and is unable to identify a compensating control or cannot find evidence to support the existence of the control, it will issue a "*finding*".
A documented finding provides for a factual description of what control objective was evaluated by the auditor. When there is an audit finding, the auditor will provide for the reasons it believes that the condition impairs the management's ability to achieve the control objectives, what is the potential root cause, what can be the **risk** and what must be done. Auditors must stay objective when issuing a finding.

Auditor's report
At the end of the audit process, the auditor will issue its audit assessment report.
The audit report is the overall assessment of the auditor of a company's management system and compliance with the standards or objectives. Generally, the auditor will outline the audit objectives and describe the methodology used to issue the report.
The auditor will also outline any possible findings it has identified along with possible recommendations on what the organization should do to remedy the finding.

Remediation
Generally, following the issuance of the systems audit report, a company should consider remediating any deviations or discrepancies discovered by the auditor.
Prepare a remediation plan and executing the plan to eliminate the root cause of what triggered a "finding" is crucial.

What is a system-based audit?
According to the Oxford Reference, a system-based audit is:

> *"An approach to auditing based on the concept that by studying and assessing the internal control system of an organization an auditor can form an opinion of the quality of the (…) system, which will determine the level of substantive tests needed to be carried out"*

This is a type of audit where the auditor's focus is the internal control system of the organization as a base to determine the type of tests and verifications needed to be carried out.

A **system-based audit** as opposed to a **risk-based audit** approach the considers risk factors and evaluates the internal controls systems based on those risks.

The system audit objectives
System audits are carried out for many objectives.
The following represents a few objectives pursued by organizations:

1. To ensure that a company's systems operate in accordance with **system standards**
2. To assess whether or not the company's systems are in **conformity** with the **system standards**
3. The evaluate the **effectiveness** of the **company's systems** to achieve its objectives
4. Allow for **system improvement** opportunities
5. Comply with **statutory and regulatory requirements**

Useful terminology
In the context of an audit process, there are some terms and terminology worth reviewing.
Here is a brief description of terms you may come across:

- Effectiveness - refers to how well the systems are working based on objective evidence and in light of defined standards.
- Findings - refers to an issue discovered by the auditors during the system audit requiring remediation or resolutions. A finding can be critical where there appears to be evidence that the systems are significantly deviating from standards or the system is not functional. A finding can be minor as well.
- Noncompliance - when there appears to be objective evidence that a company is not complying with a statute, regulation or standard and where such compliance is mandatory
- Nonconformance - when there is evidence to show that a process or system does not conform to what's required or the supporting documentation

At the end of the day, the objective of the system audit is to ensure the following:

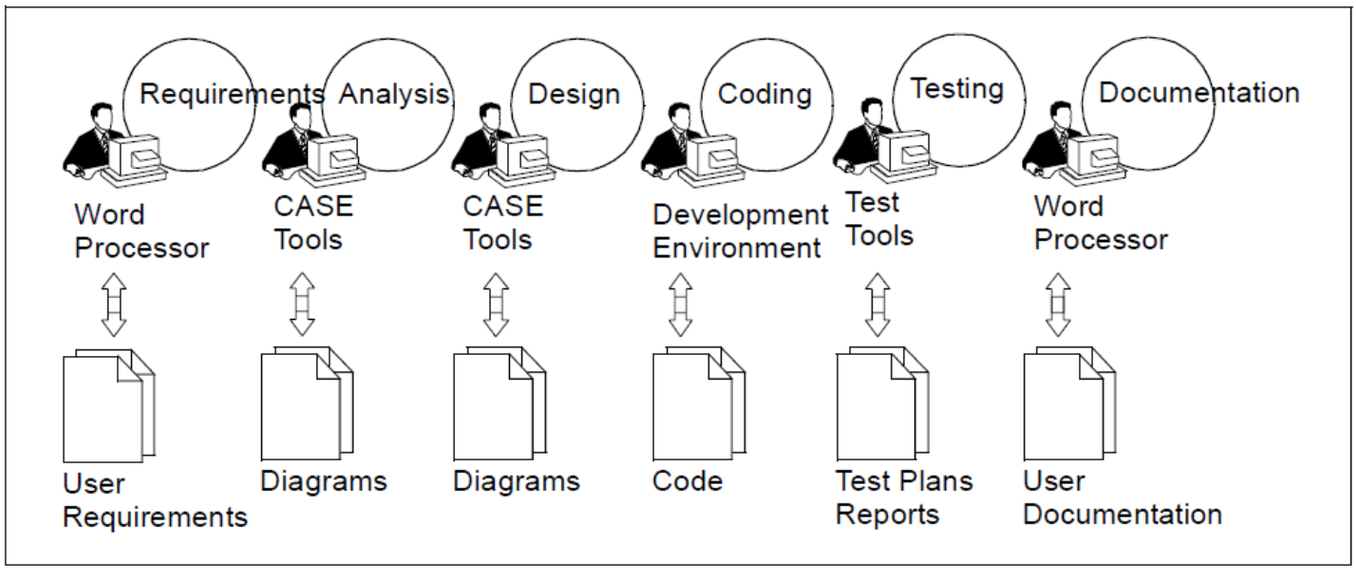
1. Evaluate the **actual performance** of their operations compared to what was **planned**
2. **Validate that the objectives** pursued by the organization remain relevant
3. Validate whether or not the company is **achieving those objectives**
4. Ensure that the systems used are **reliable**
5. Review system records to ensure systems **operate based on specifications**
6. Identify **vulnerabilities** and **risks**
7. Allow a company to define a **mitigation plan** to better achieve its objectives
8. Monitor its **operational systems** to ensure they meet the objectives on an ongoing basis

System Documentation

System documentation in all its phases is a very necessary activity often overlooked by developers and admins. Documentation in the development phases serve as a guide for future activities with the systems from re-coding to upgrades, to system administration and maintenance, and so on.

Documents are produced during the development of a software to provide a blueprint for future users. Without the documentation, people who are to deal with the software in a very technical manner would likely re-create everything. It is like users being unguided in their journey towards the software processes.

Some of the documents produced during the software development process:



Documentation on the system implementation (and administration phase) involves the write-ups that ensued in the several activities undertaken on the systems including the following:

1. Monitoring reports
2. Audit compliance
3. User management
4. Test reports
5. Incidence reports
6. Maintenance plan
7. Network plan
8. Check and inspection reports
9. Security plan
10. Integration and testing checklist

V. REFERENCES:

(2020). System Audit Basics (Understand the System Auditing Process)
https://incorporated.zone/system-audit-basics-understand-the-system-auditing-process/

Aimar, A. Introduction to Software Documentation

Frisch, E. (2018). Essential System Administration, 3rd Edition
https://www.oreilly.com/library/view/essential-system-administration/0596003439/ch01.html

Anderson, E. (2021). System Administration
http://now.cs.berkeley.edu

More, J., Stieber, A & Liu, C. (2016). Breaking into Information Security
https://www.sciencedirect.com/topics/computer-science/system-administration

VI. ASSESSMENT TASK:

DISCLAIMER

Every reasonable effort is made to ensure the accuracy of the information used in the creation of this reference material, without prejudice to the existing copyrights of the authors. As an off-shoot of the innumerable difficulties encountered during these trying times, the authors endeavored to ensure proper attribution of the esteemed original works, by way of footnotes or bibliography, to their best abilities and based on available resources, despite the limited access and mobility due to quarantine restrictions imposed by the duly constituted authorities.

We make no warranties, guarantees or representations concerning the accuracy or suitability of the information contained in this material or any references and links provided here. Links to other materials in our CPOD and CAM was made in good faith, for non-commercial teaching purposes only to the extent justified for the purpose, and consistent with fair use under Sec. 185 of Republic Act No. 8293, otherwise known as the Intellectual Property Code of the Philippines.