**SYSTEM SECURITY AND AUDIT**

**Lesson 1:**

Introduction.

What is system Security and audit

This is a protection of information systems from theft or damage to hardware, software and information as well as the disruption of services that they provide

**Objectives of learning system security and audit**

1. importance
2. Develop a strategy for pursuit of career in information security
3. Understand information security in business
4. Protects computes, networks of organizations

C. I. A (Confidentiality, integrity, authenticity, availability) - - - > goals of system security

**Goals of computer security**

1. Come up with strategies for prevention, detection and recovery of data and information
2. provide services for confidentiality, integrity, availability and authenticity

**12 principles of security**

i) there is no such thing as absolute security

-given enough time, skills and tools, a hacker can break any system security

ii) the 3 security goals (CIA) Protect the confidentiality of data,

--no unauthorized access to information is permitted and accidental disclosure of sensitive information

--Preserve integrity of data. This keeps data pure and trustworthy and protects data from intentional and accidental changes

--promotes availability of data for authorized use

iii) defense in depth of a strategy

--Implements security in overlapping layers that provide the 3 elements that secure assets.. Prevention, detection, recovery

Iv) When left on their own, people tend to make the worst security decisions

V) functionality and assurance requirement - - functionality requirement describes what a system should do while assurance requirement describes how functionality systems should be implemented and tested

What is verification? - - process of confirming that one or more predetermined requirements are met

What is validation? - - This is the correctness or quality of the mechanism used to meet the requirements stated above

Vi) security through obscurity is not an answer

vii) risk management.. Security is not concerned with eliminating all threats but eliminating known threats and minimizing loses. Risk analysis and management are central in securing systems. They place an economic value on assets to best determine appropriate counter measure that protect them from loses

Vulnerability – this is a known problem within a system or program

Exploit – this is taking advantage of a specific vulnerability or weak point

Attacker – this is the link between vulnerability and an exploit

Viii) Security controls

Security mechanism servers the purpose by preventing a compromise, detecting that a compromise is underway and responding to a compromise why it is happening or after it had been discovered.

ix) complexity is the enemy of security - - the more complex the system gets the harder it is to secure

X) fear, uncertainty and doubt do not work in selling security

XI) People. Process and technology are all needed - - this are essential elements of security practices including operations, applications, physical security, and cryptography

Xii) open disclosure of vulnerability is good for security