**UNIT-I**

**The need for information system security compliance**

1. What is a security risk assessment?

Cybersecurity risk assessment is the process of identifying and evaluating risks for assets that could be affected by cyber-attacks. Basically, you identify both internal and external threats; evaluate their potential impact on things like data availability, confidentiality and integrity; and estimate the costs of suffering a cybersecurity incident. With this information, you can tailor your cybersecurity and data protection controls to match your organization’s actual level of risk tolerance.

1. What is an IT security audit?

A security audit is a comprehensive assessment of your organization’s information system; typically, this assessment measures your information system’s security against an audit checklist of industry best practices, externally established standards, or federal regulations. A comprehensive security audit will assess an organization’s security controls relating to the following:

* Physical components of your information system and the environment in which the information system is housed.
* Applications and software, including security patches your systems administrators have already implemented.
* network vulnerabilities, including evaluations of information as it travels between different points within, and external of, your organization’s network
* The human dimension, including how employees collect, share, and store highly sensitive information.



1. What is IT compliance?

IT compliance describes adherence to legal, internal, or contractually prescribed requirements for the IT of an organization. These requirements are made up of various requirements for IT security, data protection, availability, and integrity that apply to systems and processes.

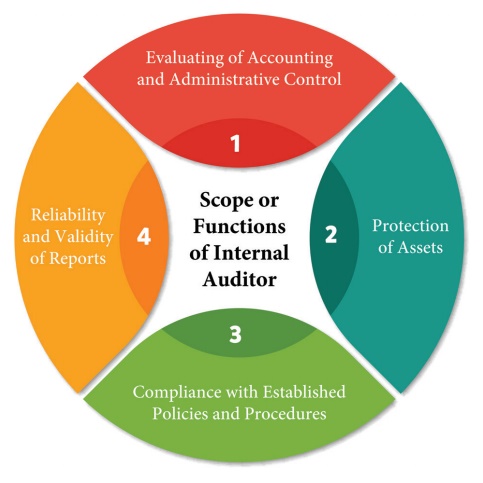
**It detects vulnerabilities, risks, and threats that organizations face and the effect of such Controls these areas.**

* Data Security – involves a review of network access control, encryption use, data security at rest, and transmissions
* Operational Security – involves a review of security policies, procedures, and controls
* Network Security – a review of network & security controls, SOC, anti-virus configurations, security monitoring capabilities, etc.
* System Security – This review covers hardening processes, patching processes, privileged account management, role-based access, etc.
* Physical Security – a review that covers disk encryption, role-based access controls, biometric data, multifactor authentication, etc.

**UNIT - II**

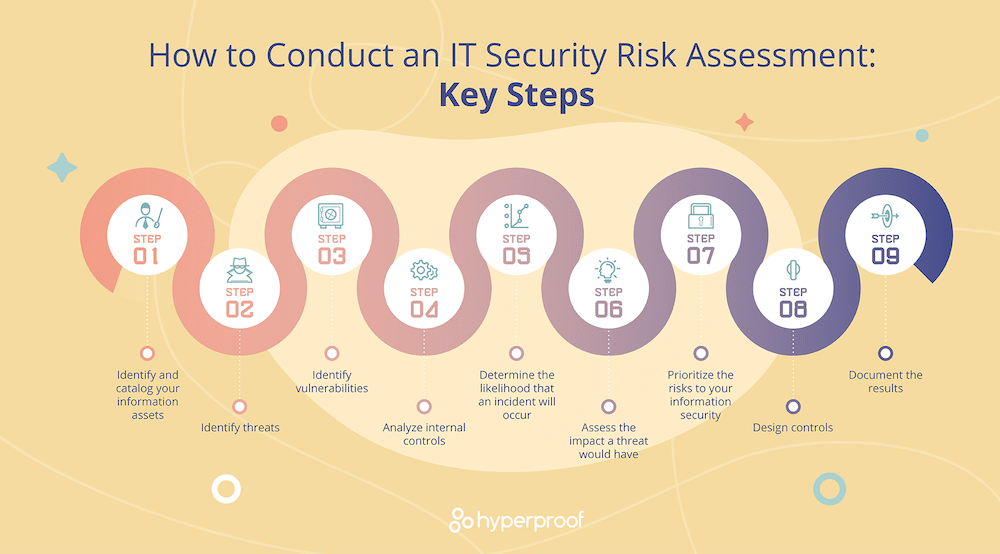
**Planning and implementation of an IT Infrastructure Audit for compliance**

* **Defining the scope for audit:**



* **Identifying critical requirements for the audit:**

Critical Audit Matters (CAM) are defined as those issues that have the potential to cause material misstatement or significant noncompliance with laws or regulations if not detected.



**7 Domains for a Cybersecurity Audit**

1. **User Domain.**  
   The User Domain covers all theusers (of any rank) that haveaccess to the other six domains.
   1. User can destroy data in application(intentionally or not) and delete all
   2. User can find that his girlfriendcheated on him and use her passwordto delete all of her work so that shewould be fired.
   3. User can insert infected CD or USBflash drive into the work computer
2. **Workstation Domain.**A computer of an individual user where the production takes place
   1. The workstation’s OS can have a known software vulnerability thatallows a hacker to connect remotelyand steal data.
   2. A workstation’s browser can have a software vulnerability which allowsunsigned scripts to silently installmalicious software.
   3. A workstation’s hard drive can fail causing lost data
3. **LAN Domain.**  
   Contains all of the workstations,hubs, switches, and routers. TheLAN is a trusted zone
   1. A worm can spread through the LANand infect all computers in it.
   2. LAN server OS can have a knownsoftware vulnerability.
   3. An unauthorized user can access the organization’s workstations in a LAN
4. **WAN Domain.**
   1. Stands for Wide Area Network and consists of the Internet and semi-private lines
5. **LAN / WAN Domain.**  
   The boundary between the trusted and un-trusted zones.The zones are filtered with a firewall
   1. A hacker can penetrate your ITinfrastructure and gain access toyour internal network.
   2. Weak ingress/egress traffic filteringcan degrade performance.
   3. A firewall with unnecessary portsopen can allow access from theInternet
6. **System / Application Storage Domain.**  
   This domain is made up of user-accessed servers suchas email and database
   1. A fire can destroy primary data
   2. A DOS attack can cripple the organization’s email
   3. A database server can beattacked by SQL injection,corrupting the data
7. **Remote Access Domain**  
   The domain in which a mobileuser can access the local network remotely, usually through a VPN
   1. Communication circuit outage candeny connection.
   2. Remote communication from officecan be unsecured.
   3. VPN tunneling between remotecomputer and ingress/egress routercan be hacked