UNIT – 3

Computer Security Audit & Compliances

Subject Teacher – Ms. Hepi Suthar

Identifying the minimum Acceptable Level of Risk

- Prioritises risk reduction
- Raises awareness of potential hazards and risks on site
- Identifies who or what may be at risk
- Quantifies potential costs any risks entail
- Highlights any shortcomings in existing risk reduction strategies
- Addresses the increase in risks over time
- Provides clear risk information for both site personnel and the public.
- **The level of Residual Risk that has been determined to be a reasonable level of potential loss/disruption for a specific IT system**.

7 Domain of IT Infrastructure

- They are as follows:
- **User Domain**
- **Workstation Domain**
- **LAN Domain**
- **LAN-to-WAN Domain**
- **Remote Access Domain**
- **System/Application Domain**.
- Each of these domains is viewed as portals for attackers if countermeasures are missing or fail. It is very imperative for businesses to protect each of these seven domains. It only takes one unprotected domain for an attacker to gain access to private data.

User domain

The User Domain covers all the users (of any rank) that have access to the other six domains.

- **RISKS:**
- User can destroy data in application(intentionally or not) and delete all
- User can find that his girlfriend cheated on him and use her password to delete all of her work so that she would be fired.
- User can insert infected CD or USB flash drive into the work computer

Workstation domain

A computer of an individual user where the production takes place.

- **RISKS:**
- The workstation’s OS can have a known software vulnerability that allows a hacker to connect remotely and steal data.
- A workstation’s browser can have a software vulnerability which allows unsigned scripts to silently install malicious software.
- A workstation’s hard drive can fail causing lost data.

LAN domain

Contains all of the workstations, hubs, switches, and routers. The LAN is a trusted zone.

- **RISKS:**
- A worm can spread through the LAN and infect all computers in it.
- LAN server OS can have a known software vulnerability.
- An unauthorized user can access the organization’s workstations in a LAN

WAN domain

Stands for Wide Area Network and consists of the Internet and semi-private lines.

- **RISKS:**
- Service provider can have a major network outage.
- Server can receive a DOS or DDOS attack.
- A FTP server can allow anonymously uploaded illegal software

LAN & WAN domain

The boundary between the trusted and un-trusted zones. The zones are filtered with a firewall.

- **RISKS:**
- A hacker can penetrate your IT infrastructure and gain access to your internal network.
- Weak ingress/egress traffic filtering can degrade performance.
- A firewall with unnecessary ports open can allow access from the Internet.

Remote Access domain

The domain in which a mobile user can access the local network remotely, usually through a VPN.

- **RISKS:**
- Communication circuit outage can deny connection.
- Remote communication from office can be unsecured.
- VPN tunneling between remote computer and ingress/egress router can be hacked

https://www.youtube.com/watch?v=OUa13H9fjug

Application domain

This domain is made up of user-accessed servers such as email and database.

- **RISKS:**
- A fire can destroy primary data
- A DOS attack can cripple the organization’s email
- A database server can be attacked by SQL injection, corrupting the data.

5 Steps to Ensuring IT Infrastructure Compliance

- A robust IT infrastructure that does not compromise on compliance is an organization’s ticket to keeping stakeholders and regulators happy.
- Complex IT environments expose enterprises to a myriad risks and threats that can throw a wrench in business operations and directly impact organizational performance.
- There is also the issue of ensuring internal compliance with departmental and corporate policies, and external compliance with the regulatory requirements in the industry.

- Compliance is all about demonstrating corporate accountability.

- Establishing well thought out IT infrastructure compliance processes and policies, guided by a clear understanding of emerging internal and external requirements, is a fail safe way of achieving this.

- Success will also depend on how well businesses are able to embed a culture of compliance across the enterprise, ensuring the support of all key stakeholders in driving the GRC mission.

Get IT GRC policies right

- Organizations need well-defined policies to drive their IT governance, risk and compliance (GRC) journey.
- Formulating integrated policies, implementing them as a series of steps, and monitoring them through checkpoints can help tighten governance and mitigate risks.
- IT GRC policies need to be implemented consistently across a spectrum of activities such as IT asset tracking, control and risk management, auditing and reporting, and incident and threat management.
- It is also essential to effectively map corporate and departmental policies to strong controls.

Embrace effective IT GRC technology

- The effectiveness of an IT infrastructure compliance strategy hinges on the efficient use of a proven IT GRC platform.
- Such a platform can help businesses breathe easy by streamlining GRC processes, simplifying compliance, and reducing the cost of compliance.
- A sophisticated technology solution for ensuring compliance also provides clear visibility into key risk indicators (KRIs), risk assessment results and compliance activities across the enterprise.
- However, organizations need to factor in domain specific integration points and trends such as Big Data analytics while choosing an effective IT GRC platform.

Achieve risk mastery

- To achieve complete control in handling enterprise-wide risks, organizations need to focus on the way IT is governed and operated.
- While Information Technology Infrastructure Library (ITIL) is considered the standard IT operations framework, GRC compliance tools can leverage ITSM activities from incident, change and configuration repositories to help organizations baseline processes and track exceptions.
- Another key imperative is implementing the right risk metrics to measure and upgrade risk practices.
- Ensuring that senior management has clear visibility and understanding of risks goes a long way in achieving IT GRC objectives.

Meet the mark with process efficiency

- As part of the IT infrastructure compliance strategy, it is important to leverage an integrated compliance framework to standardize and connect disparate processes.
- Many organizations manage governance, risk and compliance initiatives in silos, with dozens of systems performing the same set of functions.
- However, as risk and compliance initiatives become more intertwined across the organization, an integrated GRC framework can improve processes and reduce redundancies, resulting in lower costs.

Stay safe with regular audits

- The security, integrity and availability of systems and applications can be ensured through regular audits.
- A well streamlined audit management strategy also helps ascertain and ensure that IT infrastructure is in sync with industry specific compliance requirements.
- For instance, PCI and SOX in the finance industry, and HIPAA in the healthcare industry.
- By automating auditing, testing, measurement and reporting of IT controls, organizations can easily identify compliance issues, and realize further efficiencies and cost savings.