Cyber Security Audit & Compliance

What about evaluation ?

- Internal Assesment -25 x2 =50 marks
- Mid semester Examination = 50
- End semester examination = 100

Total = 200

Syllabus ?

How we shall work ? together

The need for information system security compliance

The need for information system security compliance

answer the foll. questions

- What do you mean by information ?
- How it is different from data ?
- Is data and information makes knowledge ?
- How Knowledge is different from wisdom ?
- Does our experience helps in creating knowledge ?
- What do you mean by information system ?
- Is it necessary that information system should/must be secure?

- What are security compliance ?

What is IT security Assesment ?

Security assessments are carried out by individuals who are unclear as to the **quality of the security measures** put in place on their IT systems and networks.

The benefits to a secure network are many and include the security measure's ability **to protect user confidentiality, sensitive data, system resources, and much more**.

Types of IT security Assesment

What are the types of security assesments ?

- Who can access and with what permission based
- Existing protective systems
- Compliance with security regulations
- Vulnerability to security incidents
- Resilience against potential harm

What is an IT security Audit ?

A security audit is the high-level description of the many ways organizations can test and assess their overall security posture, including cybersecurity.

Types of Audit

- Internal Audit
- External audit
- Manual audit
- Automated audit

Reference: https://www.dnsstuff.com/it-security-audit

What is compliance?

the act or process of doing what you have been asked or ordered to do.

eg.

Payment Card Industry Data Security Standard (PCI-DSS)

National Institute of Standards and Technology (NIST) Standards

https://www.webopedia.com/definitions/grc/

What is compliance?

WHAT IS THE ROLE OF A COMPLIANCE DEPARTMENT & COMPLIANCE OFFICER?

The main aim of any Compliance Department within an organization is to actively manage risk and reduce financial crime

Typically, there are five (5) defined areas of responsibility in a compliance department / officer role which include:

Identification

Prevention

Monitoring and detection

Resolution, and

Advisory

Reference: https://www.creationbc.com/news/what-is-compliance/

Audit V/s Assesment

Audit

Assesment

an examination of results to verify their accuracy by someone other than the person responsible for producing them

An assessment is a judgement made about the results.

audits are based on the quality manager’s checklist
assessments are based on formal standards and reference models
Objective snapshot in time
Educational and benchmarking
No educational components
Measurements and fedback
Completed by third party
Completed by first or second party

Why are governance and compliance important ?

What is governance ?

Governance is all the processes of interactions be they through the laws, norms, power or language of an organized society over a social system. It is done by the government of a state, by a market, or by a network.

Why governance important ?

- To preserve and strengthen stakeholder confidence
- To provide the foundation for a high-performing organisation
- To ensure the organisation is well placed to respond to a changing external environment
- Ensuring integrity and ethical behavior in the company.
- Ensuring that all shareholders are treated equitably.
- Ensuring full disclosure and transparency to all stakeholders of the company

Why are governance and compliance important ?

What is compliance ?

Compliance is the set of processes and organization uses to ensure that employees and the organization

as a whole abide by internal rules of conduct and external rules and regulations.

Why Compliance important ?

- Compliance is part of your organization's duties to its community and stakeholders.
- Without a compliance function, you cannot reliably build or maintain trust with others.
- If you have no compliance function, you invite reputational damage.
- Compliance helps define an organization's "why."
- Compliance helps define and regulate an organization's "how."
- Compliance can serve as a driver of change and innovation.
- Compliance enhances consistency.

Case Studies: 1

Branch manager denied account opening services

What are the consequences ?

Case Studies: 2

HR Manager hired his/her relative in a company

What are the consequences ?

Case Studies: 3

Paper was published in reputed journal but one staff name was not included in paper.

What are the consequences ?

What if an organization does

not comply with compliance laws?

If organization does not compliance Law ?

- Panalties
- Reputational damage
- Audits issues
- Legal action and imprisonment
- Company shut down
- Security breaches
- Impact on patient care (healthcare system)
- Wage issues
- Workplace safety
- Licensing

What is the scope of an IT

compliance audit?

What is compliance audit ?

Compliance Audit is detailed review of organization’s loyalty towards uphold of the rules and regulations which includes statutory and internal rules, regulations, policies and procedures framed by Government, local authorities and organization’s management by evaluating compliance procedure, security policies, user access control, risk management procedure and entity’s policy, procedure and processes.

What is the scope of an IT compliance audit?

What is the purpose of compliance audit ?

The purpose behind conducting a compliance audit is to assess the organization's compliance program is effective or not and bringing out the non-compliance in front of management and Government/Tax authorities.

What is the scope of an IT compliance audit?

What is IT compliance audit ?

IT Compliance is taking appropriate control of and protecting information, including how it is obtained and stored, how it is secured, its availability (how it is distributed internally and externally), and how the data is protected.

What does your organization do to be in compliance?

- Remove barriers to compliance.
- Stay on track with changing laws and regulations
- Involve specialists
- Ensure employees follow procedures
- Schedule regular internal audits
- Use the right software
- Avoiding criminal proceedings
- Assumption of social responsibility
- Assemble a compliance team
- Compliance analysis
- Formulate and communicate compliance policies
- Implementation in regular operation and adjustment
- Coordinate internal teams
- Don’t forget about international locations

What are you auditing within the IT infrastructure?

- Having outdated policies or no policies in place.
- Lack of vulnerability scanning or penetration (PEN) testing.
- Lack of an Intrusion Prevention System (IPS). Alternatively, if your IPS is not properly managed.
- Lack of two-factor authentication for any form of remote access.
- You allow your IT staff to enact as security staff and do not have a dedicated security staff.
- There is no up-to-date disaster recovery plan or tested business continuity plan.
- No data loss prevention plan in place.
- Lack of keeping up to date with OS, network or applications updates.
- Lack of a network and system drawings showing the architecture of the network as well as data flow.

Maintaining IT compliance

- Start with cybersecurity
- Take Time for Training
- Implement User Access Controls
- Encrypt Network Data

Home Work

- Consider amazon.in as information system. Identify how amazon undergoes security compliance ?
- How IT security measures are taken by FACEBOOK and GOOGLE respectively.
- If you are sent to google HQ for IT security auditing, how will you automate auditing in addition to manual auditing ?
- What is the role of compliance officer at - IBM,GOOGLE, FLIPKART and FACEBOOK

- Elaborate and write your view with scientific evidence about 3 case studies.
- What are you auditing in – Govt. Schools and ebay.in

Thank you for participation
&
contribution !