Cyber Security Audit and Compliances (Introduction)

Prepared by: Dharmesh D. Dave, Asst. Prof., NFSU

Topics Covered

- What is Audit?
- What is Compliance?
- What is Assessment?
- Difference between Audit and Assessment.
- Importance and Need of Audit
- What if an Organization does not comply?

What is Audit?

1. Audit is a process to assess and review of an organization's internal policies, controls, and activities in accordance with guideline, framework or compliances.

2. Audit can be used to assess the presence and effectiveness of IT controls and to ensure that those controls are compliant with stated policies.

3. Audits provide reasonable assurance that organizations are compliant with applicable regulations and other industry requirements.

Types of Audits:

- Financial audits
- Compliance audits
- Operational audits
- Investigative audits
- Information technology audits

Scope of an IT Audit:

- Organizational
- Compliance
- Application
- Technical

What is Compliance?

1. "The act or process of complying to a desire, demand, proposal, or regimen or to coercion." To comply is "to conform, submit, or adapt as required or requested."

2. **Two Types:** Internal Compliance and External Compliance

3. The general steps to meeting compliance include the following:

    1. Interpret the regulation and how it applies to the organization.
    2. Identify the gap or determine where the organization stands with the compliance mandate.
    3. Devise a plan to close the gap.
    4. Execute the plan.

4. Compliance is closely related to **risk management** and **governance** on all levels, be it technical, procedural, or strategic.

What is Assessment?

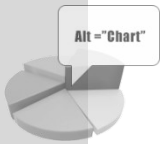
1. An IT security assessment is a key activity that involves the management of **risk** — an uncertainty that might lead to a loss.

2. " Assessment is an evaluation process against the security perimeters and controls in the organization with respect to the standard or compliance. "

3. A risk-based approach to managing information security involves the following:
   - Identifying and categorizing the information and the information systems
   - Selecting and implementing appropriate security controls—actions or changes to be applied to systems to reduce weaknesses or potential losses
   - Assessing the controls for effectiveness
   - Authorizing the systems by accepting the risk based upon the selected security controls
   - Monitoring the security controls on a continual basis

Methods of Assessment:

- Examination
- Interview
- Test

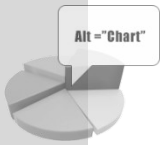


Assessment v/s Audit

1. Assessment is one part of the Audit. Because Audit provides an assurance to the organization.

2. Audit findings might place blame on specific individuals or groups within an organization. Assessments, on the other hand, are nonattributive.

3. The consequences of failing an audit can create a sense of fear, whereas an assessment simply identifies gaps to improve security operations and achieve goals.

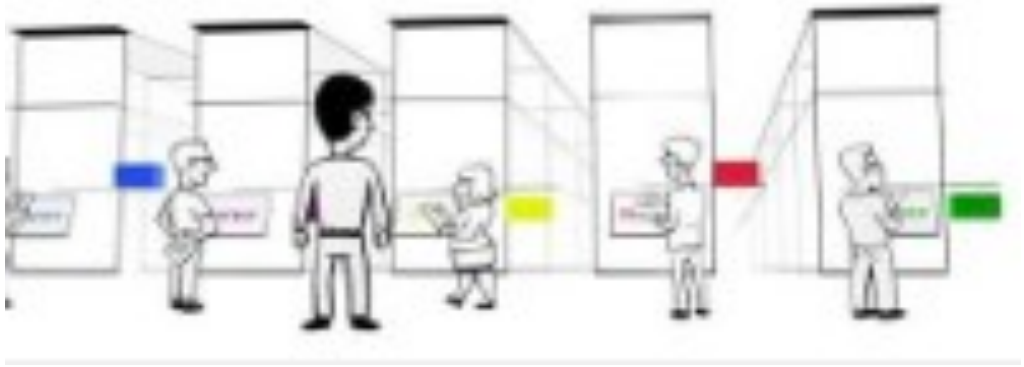


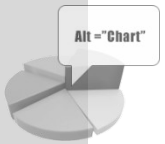
Importance and Requirement of Audit

1. Audit is required to safe organization's IT assets, Data and Reputation from the cyber attackers. Also to be saved from law/compliance penalties.

2. Audit provides a report stating the observations and gaps with the security controls, design, application or system which can be patched or implemented in order to make the organization more robust against the cyber attacks.

3. Audit can also provide the best budget solution to invest smartly in the security after the assessment and the findings.





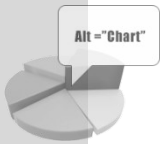
Auditing Advice

1. Auditors should never be involved in the auditing of processes, systems, or applications that they themselves designed or implemented.

2. Audits are an independent evaluation. A security assessment may also be conducted independently, but it is not necessary. Many organizations use a combination of both.

3. Audits follow a rigorous approach and are conducted according to accepted principles. This also requires that auditors be qualified. The approach taken for an assessment can fall across a wide spectrum, but in many cases, they have taken a cue from audits with well-defined approaches and frameworks.

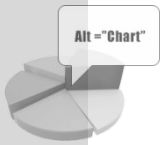
4. In the event an organization passes an audit, the organization typically receives some type of certification or confirmation. This is not the case for assessments.



What If organization does not Comply?

1. Compliance is subject to various types of industrial and organizational sectors. i.e. Bank, ICS, IT company, Govt. org, Hospitals, Financial org., etc.

2. Different compliance has different penalties in terms of money, license, etc.



Case Study…

Any Questions?

Let's Go for the next Topic.