CYBER SECURITY, AUDIT & COMPLIANCE

Date ___/___/___

IT SECURITY ASSESSMENT

Four step of a successful security risk assessment model:-

(i) Identification – Identifying the assets.
- Who all we are working with?
- How much information we are dealing with?

(ii) Assessment – Analyzing the threats.

(iii) Mitigation – Applying the security techniques to solve the security threat.

(iv) Prevention – Implement tools & processes to prevent threats.

Problem solved by Security Risk Assessment:-

(i) Identification of Assets i.e. • Built up network • Servers • Application • Data Centers • Tools.

(ii) Create Risks Profile for each assets.

(iii) Understand what data is stored, transferred or generated by these assets.

iv) Measure the risk ranking for assets and prioritize them for assessment.

v) Apply mitigating controls for each assets based on assessment results.

Page No.

Q.) Why is Security Audit Needed?

Ans. - To identify the security gaps, problems & weakness.
- Establishes a security base line that future audits can be compared with.
- Helps in organizing security policies for companies.
- Comply withe external regulatory environments.
- Identify inadequate resources.
- Determine if security trainings are adequate.

Q.) When is security audit needed or required?

Ans. It happens quaterly or in six months depending on how big or small the resource is. For ex:-
TCS has a building at location X which is very much bigger and greater than the building at location Y. So, the building X will have a security audit quaterly whereas building at location Y will be audited either in six months or yearly.

Q.) What systems does your auditor covers?

Ans. - Network Vulnerability
- Security Controls
- Encryption
- Software Systems
- Architecture Management & Capabilities
- Telecommunication Control
- Systems Development Audit
- Information Processing.

Date ___/___/___

Steps Involved in a Security Audit

1) Agree on goals. (Achievement to made in the Audit)
2) Define the scope of an audit (which all assets to audit).
3) Conduct the audit and identify threats.
4) Evaluate security and risks. (Method to be used)
5) Determine the needed controls. (How to solve threats).

Compliance Audit

It is the detailed review of the organizations rules and regulations framed by government local authorities and organization management.

What are the objectives?

- To ensure that the company meets or follows the government guidelines.
- To improve the organization efficiency.
- To uphold the faith of stakeholders.
- To comply with various other laws like environmental law, waste law, consumer safety law.
- To ensure Standard Operating Procedure (SOP) is being followed.

★ Compliance Audit Process :-

- For an organization :-
  - Identify the need & extent of the audit.
  - Select the auditor, verify the auditor, meet the qualification criteria for conducting an audit.
  - Cordinate with the auditor with all the requirements and information asked.

Page No. ___

- For an auditor :-
  - List out the laws applicable for the entity.
  - Obtain the list of companies internal policies, procedures and descisions.
  - Engage the experienced team members, older employees for the assignment.
  - Segregate the different areas of the organization to audit.
  - Obtain the list of laws applicable to entity and their compliance status.
  - Plan the audit, natrue, extent, timing, and procedures to be performed.

TYPES OF AUDIT OR COMPLIANCE AUDIT :-

- SOC 2 - Compliance Certificate which cloud has to abide by.
- ISO27000 Series - Applicable to organization managing the security assets of third parties.
- GENERAL DATA PROTECTION REGULATION :- applies to companies that process the data of European citizen.
- SAR VANS OXLEY - applies to public companies that issues IPO.
- PCI Compliance Standards - applicable to companies providing credit card & payment services.

Date ___/___/_____

- HIPAA COMPLIANCE REGULATION:- Applies to Health care facilities.
- FINRA :- Applies to Investment Industry, Stock Brokers, Broker Dealers.
- FISMA :- Applies to US governmental Organization. (FEDERAL INFORMATION SECURITY MANAGEMENT ACT)
- OBLIGATORY COMPLIANCE AUDIT :- Any organization that wants to conduct an audit can do so by appointing any person who meets the qualification criteria.

Q. Who does the compliance Audit perform?
- Whoever is eligible.
- Company's Internal Auditor team
- Team of External members
- Person mentioned in the law by the organization.

IMPORTANCE OF COMPLIANCE
- Identify weakness in the regulatory compliance process
- It helps to reduce the risk.
- Helps to develop the faith of stakeholders.
- Ensures that all the laws are being followed.
- Non-compliances can be corrected or identified.

Page No. ____

Diff. b/w compliance & Financial Audit:

- Financial Audit can be done by a single person whereas for compliance there is whole team involved.
- Financial Audit can be done by only CA whereas anyone eligible can do security audit.

Q. What if an organization does not comply with compliance laws?

- It occurs when organization fails to comply with policies standards regulations or law relevant to its operations.
  Ex:- To wear personal protective equipments.
- Insufficient administration of operations.
- Failure to obtain proper certification or illegal operation
- Failure to follow operation procedures.
- Failure to report to relevant authorities.

★ Drawbacks of Non-Compliance.

- Required by the law.
- Audits (If non-compliant, unnecessary audits have to be done.)
- Financial Penalties. (Heavy fines to be imposed)
- Imprisonment
- Brand value & Market Reputation (will go down)
- Forced shutdown of the company.

Page No.

H.W Date ___/___/___

Case study

Q.) What does your organization do to be in compliance?

Q) Diff b/w Audit and Assessment.

- An audit is an examination of results to verify accuracy by someone other than the person responsible.
- An assessment is a judgement made about the results.

Page No.