17/09/2023

Cybersecurity Audit and Compliance:

Q1. What is an IT security Assesment?

1. Part of larger security program within an org.
2. Key activity that involves management of risk.
3. Risk based approach:
   i) Identifying & categorizing info and systems
   ii) Selecting and implementing appropriate security controls.
   iii) Assesing controls for effectiveness.
   iv) Authorizing the system by accepting risks based upon the selected security controls.
   v) Monitoring security controls on a regular basis.
4. This approach is a continuous cycle.
5. Security controls include physical, procedural, tech mechanisms to safeguard systems.
6.
7. A secAssesment should produce info required to do the following:
   i) identify weakness within implemented controls
   ii) confirm that previous weaknesses are mitigated
   iii) Prioritize further decisions to mitigate risk.
   iv) Provide Assurance.
   v) Provide support for future budgetary requirement
8. NIST Framework for effective security assesment in NIST Special Publication 800-53A
   • They contain recomended procedures, which ind set of assesment objectives or goals. Each object has set of assesment ~~procedures~~. methods ind specification mechanism activity

NIST Special Publication: 800-53A

↓

Reccomended Procedures

↓

Set of Assesment objectives/goals

↓

Set of Assesment objects

↓

Specification, Mechanism, Activity, Individual.

- Assesment objectives:

→ To check are there controls applied for various things.

- We can use several methods to conduct an assesment of security controls:

i) Examination:
ii) Interview
iii) Test.

- Sample assesment we might encounter:

i) Network Security Architecture review
ii) Review of security policies, procedures, practices
iii) Vuln scanning and testing
iv) Physical security assesment.
v) Social engineering assesment.
vi) Application assesment.

Q2. IT Security Audit:

- It is an independent assesment of an organization's internal policies, controls and activities.
- Use audit to assess the presence and effectiveness of IT controls and to ensure that those controls are

compliant with stated policies.

- The scope of an IT Audit often varies, but can involve combination of the following:

i) Organizational: examines management control over IT and related programs, policies & processes.

ii) Compliance: pertains to ensuring that specific guidelines, laws, requirements are met.

iii) Application- involves apps that are strategic - eg those used by financial companies.

iv) Technical: examines IT infra and data comms.

An effective IT security audit program should ultimately accomplish 3 goals:

1. Provide an objective and independent review of an org's policy, information, systems, controls.
2. Provide reasonable assurance that appropriate and effective IT controls are in place.
3. Provide recommendations for both corrective actions and improvement to controls.

Q3. What is compliance:

IT Compliance

Internal	External
Org's ability to follow its own rules which are based on its policies	• need or desire for an org for an org to follow rules & guidelines. set forth by org's and initiatives. • Few are guidelines standards, whereas few are compliance mandate regulatory in nature.

- In most of the cases, regulations do not provide specifics and are open for interpretation.
- Compliance frameworks like COBIT and standards such as NIST, help interpret how to comply with the regulatio
- The general steps to meeting compliance include the following:

i) Interpret theregulation and how it applies to the organizat
ii) Identify the gap - where it stands to compliance mandate.
iii) Make a plan to close the gap.
iv) Execute the plan.

- closely related to risk management and governance at all levels.

Risk Management	Compliance:	Governance
eeks to mitigate risk through controls	Helps RMgmt by verifying that the desired controls are in place	seeks to better run an org using comp and accurate ins and mgmt processes or controls

4. How Audit Differs from Assesment?

i) Failure : Audits are clear and state : Pass / Fail.
Assesments are seeing where you are and making improvements as necessary.

ii) Blame:

iii) Consequences: Audit can have consequences out of which most are negative. Failing an audit can have blame attributed to an individual or group. non-compliance with regulatory mandates and standards can lead to hefty fines and legal action.

- Security auditing in general, must follow a more rigid approach and process over a security assesment. Especially when we think / consider audit as assesment. Few unique characteristics of an audit

1. An auditor should never engage in a audit of processes, systems, applications ~~that~~ designed / implemented by them.
2. Audits are independent evaluation.
3. Audits follow a rigorous approach and are conducted according to accepted principles. This also requires the auditors to be qualified. Approach used for assesment can have cues from audits with well defined approaches and frameworks
4. Org will get a certifications / confirmation incase they pass the audit. Not the case for assesment
5. Audit is concerned about past results and performance whereas assesment considers previous and current results as well as expected performance.

Q5. Why are governance and compliance ~~and~~ are Imp?

- Without proper governance, an organization can neither have effective risk management nor compliance.
- At a fundamental level, internal compliance to corporate policies is critical to the success of any business.

Q6. What happens if an org does not comply with compliance laws:

- Negative effects that non-compliance can have on an organization, beyond the threat of fine and imprisonment
1) legal fees resulting from infringements contained within many regulations
2) Brand image loss revenue as customers abandon a business.
3) Negative effect upon stock price, hurting shareholder value.
4) Increases cost of capital.

- Some regulations are strict liability, means even if there was no intent, government agencies can levy hefty penalties and time in jail.

Q7. What org must do to be in compliance?

- Achieving compliance with external standards and regulations must be your first consideration in assembling a policy infrastructure.
- Not just technical, non technical too.
- A good starting point with a solid organizational governance framework. Frameworks like COBIT provide a blueprint for implementing high level controls. Further, control standards such as ISO/IEC 27002 and NIST 800-53 provide more specific security controls.
- Understand what is applicable. Address risks.
- Perform gap analysis.

4. Protecting and Securing Privacy data.
- American Institute of Certified Public accounts

AICPA defines privacy management as "the right and obligations of individuals and orgs collection, use, disclosure and retention of personal information".

Methods to protect privacy data:

1. Develop appropriate privacy policies
2. Establish the position of privacy officer.
3. Conduct trainings of people.
4. Consider adequate controls around data retention and data destruction
5. Conduct regular risk assesment of access controls
6. Limit data to only that which is required.
7. Consider security technologies such as encryption.

Popular examples of privacy laws:

1. HIPAA (Health Insurance Portability and Accoun Act) - Privacy Rule, TiHe II - Sec and priv of heal
2. Gram Leach Bilely Act (GLBA) - Financial Priva Rule - concerned with collection and disclosure of personal financial information.
3. Children's Online Privacy Protection Act (COPPA) Provisions for apps collecting data from children below age 13
4. National Do Not Call Registry:
5. SB1386 - California Security Breach Information Act regulates privacy of personal info.

6. Electronic communications privacy act. 2000

7. Privacy act of 1974

8. The Fair Credit Reporting Act.

9. Personal Info Protection and Electronic Docs Act (PIPEDA) - Canadian law

3. Designing and Implementing Proper security controls:
The process of selecting security controls needs to be a part of an overall framework for risk mgmt, For example, the following activities consider the implementation of controls within the context of such a framework:

1. Discover and classify data and information systems. First consider CIA of data and info systems. Next, examine the potential impact on the organization if CIA was compromised.
2. Select appropriate security controls.
3. Implement security controls.
4. Asses Security controls.
5. Authorize controls.
6. Monitor the controls.

Q8. What are you auditing within the IT infra.?

Across the infra, an audit should primarily focus primarily on these 3 objectives:

1. Examine existence of relevant and appropriate security policies procedures.
2. Verify the existence of controls supporting the policy.
3. Verify effective implementation and ongoing monitoring of controls.

A. The seven domains of a typical IT infrastructure

1. LAN Domain: The equipment that makes up the LAN. A LAN is a CN for communications between the systems covering a small physical area.
2. LAN to WAN domain: Bridge between LAN-WAN
3. WAN Domain: The equipment & act beyond the LAN-WAN domain and outside the LAN.
4. Remote Access Domain: The access infrastructure for users accessing remote systems.
5. System / Application Domain: Sys on network that provide the apps and software for the users.
6. User Domain : The end users of the systems including how they authenticate into the sys
7. Workstation domain: The end user's OS. operating environment.

Q9. Maintaining IT compliance:

At minimum:

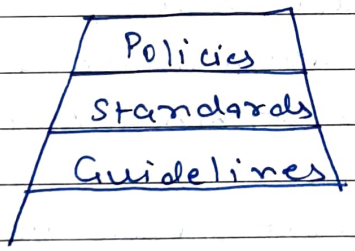
- Regular assesment of selected sec control
- Configuration and control management process
- Change management process
- Annual audit of security env.

1. Conducting Periodic Security assesments
   i) i) High Level SA
   ii) Comprehensive SA
   iii) Preproduction SA

2. Performing an Annual Security compliance audit

3. Defining proper security controls.

4. Create an IT security policy framework.



5. Implementing SOC and Admin mgmt.

6. Configuration and change management.