1/9/22

* What is Audit?

→ • Audit is a process to assess and review of an organizations internal policies, controls and activities in accordance with guideline, framework or compliances.

• Audit can be used to assess the presence and effectiveness of It controls & to ensure those controls are compliant with standard policies.

• 160 controls

• It gives an assurance.

• Scope → Technical, Strategic

• Audit provide reasonable assurance that organizations are compliant with applicable regulations and other industry requirements

IT Scope of Audit - Organizational, compliance, Application, Technical

* Compliance:

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

whatever written in an act you are obeying that is a compliance whether complying or not (mean following or not)

Two types

- Internal compliance
- External compliance.

Internal audit External audit

Steps to meeting Compliance:

1. Interpret the regulation & how it applies to the organization.
2. Identify the gap. → [existing gap → observation]
3. Devise a plan to close the gap.
4. Execute the plan.

- Compliance is closely related to risk management and governance on all levels, be it Technical, Procedural or strategic.

* What is Assessment? (Is a part of Audit)
  - Is a key activity that involves the management of a risk - an uncertainty that might lead to a loss.
  - Is an evaluation process against the security parameters and controls in the organization with respect to the standard or compliance.

* Whether controls you have are truly effective → it is an assessment

Risk based approach to manage IT security:-
1. Identify and categorize info & information systems
2. Selecting and implementing security controls
3. Assessing the controls
4. Authorizing: Authorizing the systems by accepting the risk based on selected security controls.
5. Monitoring the security controls on continuous basis.

21/9/22

- Compliance goes beyond just conforming to internal policies and standards. Compliance extends outside of the organization mapping to external regulations and industry standards.
- Regular assessments and audits of the IT environment are important for ensuring compliance.

Types of Audits

- Financial Audit -
  Determine whether an organizations financial statements accurately and fairly represent the financial position of the organization.
- Compliance audits -
  Determine if an organization is adhering to applicable laws, regulations and industry requirements.

- Operational audits -
  Provide a review of policies, procedures and operational control across different departments to ensure processes are adequate.

- Investigative audits -
  Investigate company according processes based on suspicious activity or alleged violations.

- Information technology audits -
  These address the risk exposures within IT systems and assess the controls and integrity of information systems.

Scope

It means a boundary where we require an audit There are :-

1) Organizational → This examines the management control over IT and related programs, policies and procedures.

2) Compliance → This ensures that the regulations, rules or requirements have been met.

3) Application → This involves the applications that are strategic, the eg those typically used by Fortune 5 operation.

4) Technical → This examines the IT infrastructure & data communications.

* Three goals an effective IT Security audit program should accomplish:-

1) Provide an objective and independent review of an organizations policies, information systems and controls.

2) Provide reasonable assurance that appropriate and effective IT controls are in place.

3) Provide audit recommendations for both corrective actions & improvements to controls.

Methods of Assessment

1. Examination - Verify, inspect or review associated assessment objects to understand or obtain evidence to support the existence and effectiveness of the security control.
   Eg:- • Reviewing security policies & procedures
   • Observing physical security mechanisms.

2. Interview - Discuss associated assessment objects with group or individuals to understand or obtain evidence to support the existence & effectiveness of security control.
   Interview include → Senior officers, system owner, security officers, n/w admin etc.

3. Test - Put associated assessment objects under specific conditions to compare actual behaviour with what is expected to obtain evidence to support the existence & effectiveness of the security control.
   Objects can be hardware or s/w.
   Eg:- Penetration testing, testing actual security configuration.

Types of assessment:-
- N/w security architecture review
- Security risk assessment
- Vulnerability scanning & testing
- Application assessment
- Physical security assessment.
- Social engineering assessment etc.

Difference between Audit & Assessment?

- Assessment is a part of Audit.

Failure → . It is possible to fail an audit. Audits are more clear cut in sense of pass & fail.
- Assessment is an opportunity to assess the current state and make improvements as necessary.

Blame :- . Audit findings may blame on specific individuals or group.
- But Assessment they don't view an individual directly responsible for a poor finding.

- Many organizations use assessments to prepare for audits.
- Assessment provide a chance for improvement

Consequences - - Audit can mostly have negative consequences.
- Penalties
- The consequence of failing an audit can create a sense of fear whereas an assessment simply identifies gaps to improve security operations & acheive goals.

What if organization doesnot comply?

⇒ Compliance is subject to various types of industrial and organizational sectores. ie Bank, ICS, IT company, Govt org, Hospitals, Financial org

Different companies get different penalties in terms of money, license etc.

Beyond threat of fines or imprisonment there are other issues that non compliance can have.
- Legal fees resulting from infringements contained within many regulations.
- Brand damage
- Negative effect upon stock price, hurting shareholder value.
- Increases in the cost of capital.

* It can result in huge fines as well as jail time.
* Other than financial and reputational consequences they also experience operational consequences

ISO/IEC standards

International organization for standardization is a non governmental group that brings both the private & public sectors together & creates SITUS for business & society

ISO/IEC 27000 is a series of standards & related terms that provide guidance on matters of information security. This include implementation designing, auditing an information security management system (ISMS)

ISO - standards

1. Information Security Policy

Objective :- To provide management direction and support for information security based on business requirements & other rules and regulations.

i) Policies for information security:-

Control :- A set of policies for information security should be defined, ~~manage~~ approved by management, published and communicated to employees & relevant third party.

ii) Review of the policies for information security :-

Control :-

The policy of information security should be reviewed at particular intervals or if significant changes occur to ensure their continuing suitability, adequacy and effectiveness.

2. Organization of Information Security

Internal organization :-

objective :- To establish a management framework to initiate and control the implementation and operation of information security within the organization.

i) Information security roles and responsibilities :-

Control :- All info security responsibilities should be defined & allocated.

ii) Segregation of duties :-

control :- Conflicting duties and areas of responsibility should segregated to reduce opportunities for unauthorized or unintentional modification or misuse of organizations assets.

iii) Contact with Authorities :-

Control - Appropriate contacts with relevant authorities should be maintained.

iv) Information security in project management :-

Control :- Information security policy should be addressed in project management regardless of type of project

Mobile devices and teleworking

Objective :- To ensure the security of teleworking and use of mobile devices.

i) Mobile device policy :-

control :- A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

ii) Teleworking :-

Control :- A policy and supporting security measure should be implemented to protection of information accessed, processed or stored in teleworking sites.

2

Asset management

* Responsibility for assets :-
Objective: To identify organizational assets and define appropriate protection responsibilities.

i) Inventory of assets

Assets associated with information and information processing facilities should be identified and an inventory of these assets should be drawn up and maintained.

- ~~Role lifecycle of asset (creation, processing,~~ info
- Asset inventory should be accurate, up to date, consistent and aligned with other inventories.

ii) Ownership of assets

Assets maintained in the inventory should be owned

- Individuals as well as other entities having approved management responsibility for the asset lifecycle qualify to be assigned as asset owners.

- Asset owner should ensure: the assets are inventoried, appropriately classified and protected etc.

iii) Acceptable use of assets :-

Rules for acceptable use of information and of assets associated with info and info processing facilities should be identified, documented and implemented.

• Employees and external third party users using or having access to the organization's assets should be made aware of the information security requirements of the organization's assets associated with information & info processing facilities and ~~processing~~ resources.

iv) Return of assets :-

All employees and external party users should return all of the organizational assets in their possession upon termination of their employment, contract or agreement.

• During the notice period of termination, the organization should control unauthorized copying of relevant information by terminated employees and contractors.

* Information classification :-

Objective: To ensure that information receives an appropriate level of protection in accordance with its importance to the organization.

i) classification of information:-
Information should be classified in terms of legal requirements, value, criticality and sensitivity to unauthorized disclosure or modification.

ii) Labelling of information:-
An appropriate set of procedures for information labelling should be developed and implemented in accordance with the information classification scheme adopted by the organization.

iii) Handling of assets:-
Procedures for handling the assets should be developed and implemented in accordance with the info classification scheme adopted by organization.
- access restrictions based on classification
- maintanena of record of authorized recipients of assets.
- Storage of IT assets in accordance with manufacturers specifications etc.

* Media Handling:-

Objective: To prevent unauthorized disclosure, modification, removal or destruction of info stored on media.

i) Management of removable media :-

procedures should be developed and implemented for management of removable media in accordance with the classification policy of organization.

- Registering of removable media.
- Keeping multiple copies of same data (in case of data loss)
- Using cryptographic techniques while storing
- If no longer required, make them unrecoverable.
- All media should be stored in safe, secured place along with manufacturer's specification.

ii) Disposal of media :-

Media should be disposed securely when no longer required, using formal procedures.

- Incineration, shredding
- Formatting
- overwriting (upto 4 times)

iii) Physical media transfer :-

Media containing information should be protect against unauthorized access, misuse or corruption during transportation.

- reliable transports or couriers should be used
- Packing securely etc.

ISO - standards

Access Control

* Business requirements of access control:-
Objective:- To limit access of information and information processing facilities.

i) Access control policy:-
An access control policy should be identified, documented and implemented in accordance with business & info security requirements.

- Asset owners should determine appropriate access control rules, access rights & restrictions for users of specific roles towards their assets.
- Access controls are both logical and physical and these should be considered together.

ii) Access to n/ws and n/w services:-
Users should be given access to n/w and n/w services that they have been specifically authorized to use.

* User access management:-
objective:- To ensure authorized user access and to prevent unauthorized access to systems and services.

2

i) User registration and de-registration:-

A formal user registration and de-registration process should be implemented to enable access rights.

- Giving unique user id's
- Immediatly disabling or removing user id if user left organization.
- ensuring redundant user id's not shared to others etc.

ii) User access provisioning:-

A formal user access provisioning process should be implemented to grant or revoke access rights to all users for all systems.

The provisioning proces include:-

- obtaining authorization from owner of info system to use it
- maintaining central record of access rights of each user id.
- ensuring access rights not activated before authorization.
- verifying access level is appropriate to access policies & other requirement like (segregation of duties).
- periodically reviewing access rights.

3

iii) Management of privileged access rights:-

The allocation and use of privileged access rights should be restricted & controlled.

iv) Management of secret authentication information of users:-

The allocation of secret authentication information should be controlled through a formal management process.

- Users should sign a statement - to keep personal secret authentication info secret.
- ~~Before~~ when users need to maintain this info they should initially given a temporary info which they are forced to change. (Eg: password)
- Should be unique & shouldn't be guessable.
- Before changing verify the user etc.

v) Review of user access rights:-

Asset owners should review user's access rights at regular intervals.

vi) Removal or adjustment of access rights:-

The access rights of all employees and external parties to info & info ~~security~~ processing facilities should

be removed upon termination of their contract, agreement or employment or be adjust upon change.

* System and application access control:-
objective:- To prevent unauthorized access to systems and applications.

i) Information access restriction:-
Access to information and application system functions should be restricted in accordance with the access control policy.

- controlling access rights to users.
- controlling access rights to other applications.
- controlling which data can be accessible by particular user.

ii) Secure log on procedures:-
where required by access control policy, access to systems and applications should be controlled by a secure log on procedure.

iii) Password management system:-
Password management systems should be interactive and should ensure quality passwords.

iv) Use of privileged utility pgms:-

The use of utility programs that might be capable of overruding system application controls should be restructed and tightly controlled.

v) Access control to program source code:-

Access to program source code should be restricted.

Cryptography

* Cryptographic controls:-

Objective:- To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information.

i) Policy on the use of cryptographic controls.

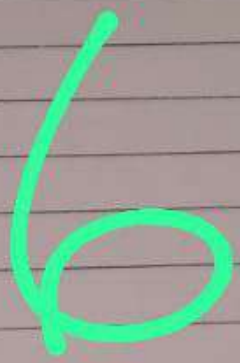
A policy on the use of cryptographic controls for protection of info should be developed and implemented.

ii) Key management:-

A policy on the use, protection & lifetime

of cryptographic keys should be developed and implemented through their whole lifecycle.

The policy should include requirements for managing cryptographic keys through their whole lifecycle including generating, storing, archiving, retrieving, distributing, retiring and destroying keys.



```
#!/bin/bash
mkdir $1
echo "Directory named $1 is created"
```

* While running give ./first.sh abc

Audit 16/11/2022

* UPS

Types of UPS - 1) Online → Automatically turns on when power goes off (in fraction of second)
& Offline → operated manually

2) Modular → You can add more batteries (Enhancement space is there)
& static → Fixed ₹.

Capacity is measured in KW

* Generator set
  - Automated & Manual.

* Power.

* Rack

PDU → Power Distribution Unit

Rodent control → Pest control
Dedicated system based on sensors.

* Camera → fixed →
OR
Panning → can move/rotate

Backup 3 months min on the disk.
Stored back → 1 year.

* Maintenance.

N/w architecture

Types of switches → L2 L3
↓ ↓
Layer 2 Layer 3

Normally switch work on layer 2. But there are switches which can work on both layers.
→ Manageable/unmanageable

Humidity control?

Backup procedures?

DR? Disaster Recovery sites.

Location of Datacenter

Load Bearing capacity?

Seismic zones

A.C.

Operations Security

- change management →

Change → change into an application,
Eg: the finance manager need some changes in the normal application (some automated works)
If a vulnerability cause (If he didn't informed the in-house)

Change requisition form.

CIA → confidentiality, Integrity, Availability

AAA → Authorization, Authentication, Accountability

UAT ⇒ User Acceptance testing → Alpha
→ Beta.

Development Env.
• Engineer → Deployment

Development Env.
UAT environment
Deployment environment / production env

UAT Env should be identical to deployment environment. (Blame last)

N/w architecture

Types of switches → L2 L3
↓ ↓
Layer 2 Layer 3

Normally switch work on layer 2. But there are switches which can work on both layers.
→ Manageable/unmanageable.

Humidity control?
Backup procedures?
DR? Disaster recovery sites.
Location of Datacenter
Load Bearing capacity.

cysmic zones

Acc.

VIU

Operations Security

- change management →

Change → change into an application,
Eg. the finance manages need some changes in the normal application (some automated works)
If a vulnerability cause (if he didn't unfoomed the intranet)

Change requisition form.

CIA AAA
↓ ↓
Confidentiality Authorization
Integrity Authentication
Availability Accountability

UAT ⇒ User Acceptance testing → Alpha → Beta.

- SEngineer → Deployment

Development Env.

Development Env:
UAT environment
Deployment environment / production env

UAT Env should be identical to deployment environment. (Bdame last)