Domain 6

Security Assessment & Testing

Audit

Test against standards

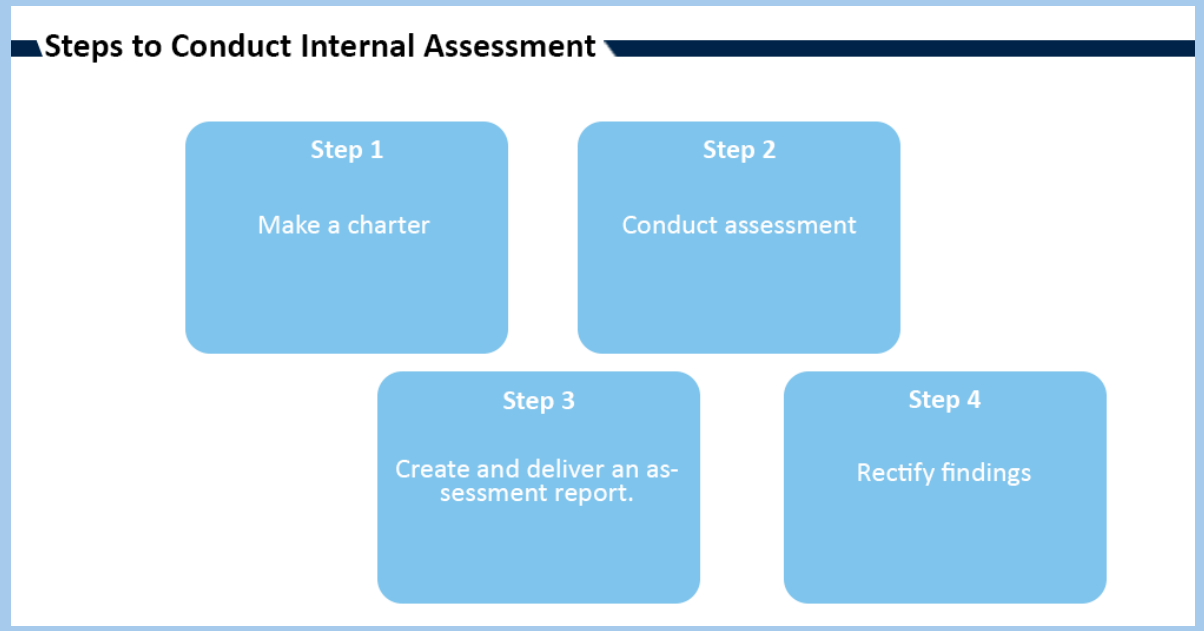
PCI-DSS, HIPAA

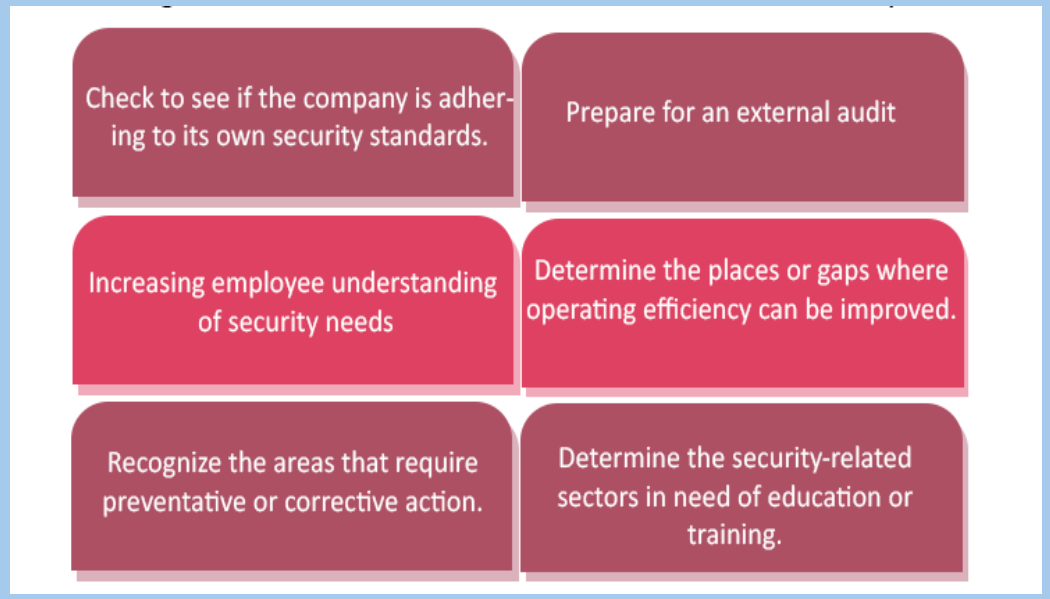
Detective control

An audit is an evaluation carried out by an independent third party to show that the organization's procedures and controls adhere to a compliance standard.

Internal Audit

- Done by internal Team
- Convenience
- Conflict of Interest





External Audit

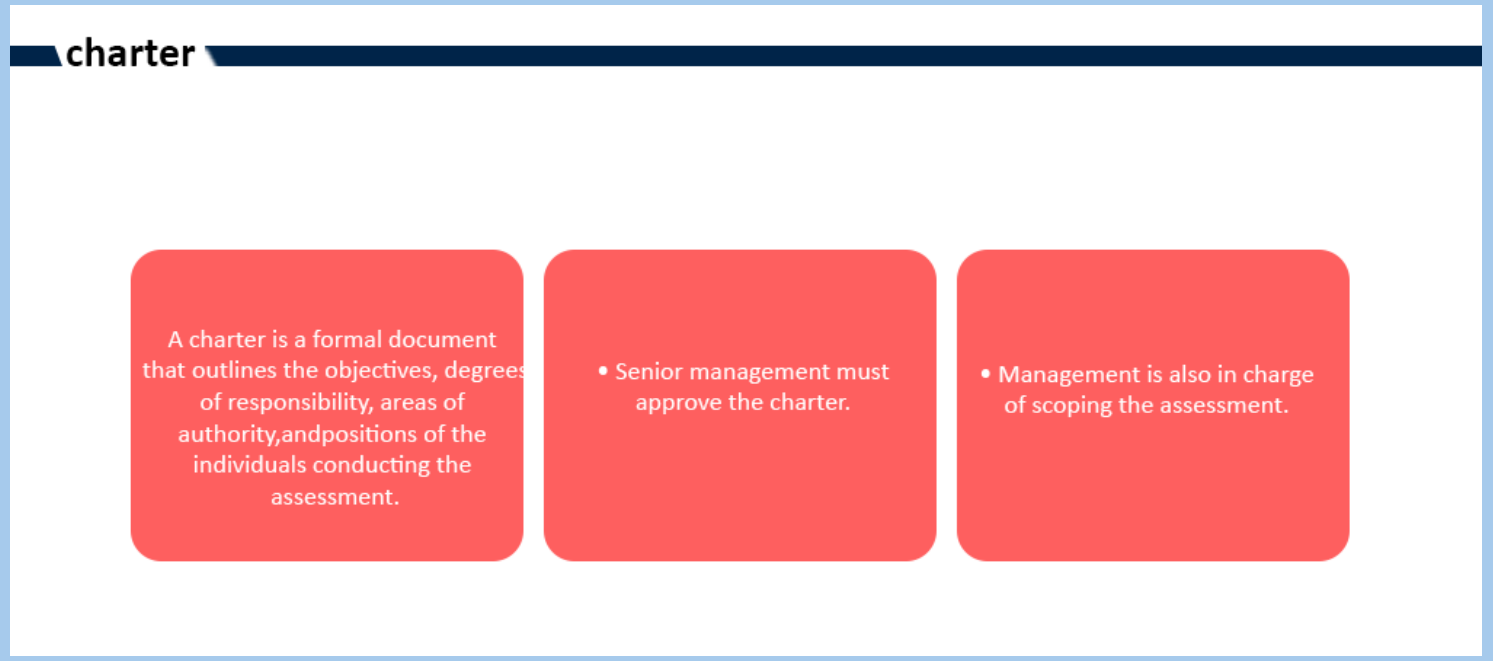
- No conflict of interest
- Costly
- 3rd Party – all Controls related to 3rd party should be implemented

An audit is an evaluation carried out by an independent third party to show that the organization's procedures and controls adhere to a compliance standard.

Not compliance could have negative effects such as fines, legal action, restrictions on one's ability to conduct business, and more.

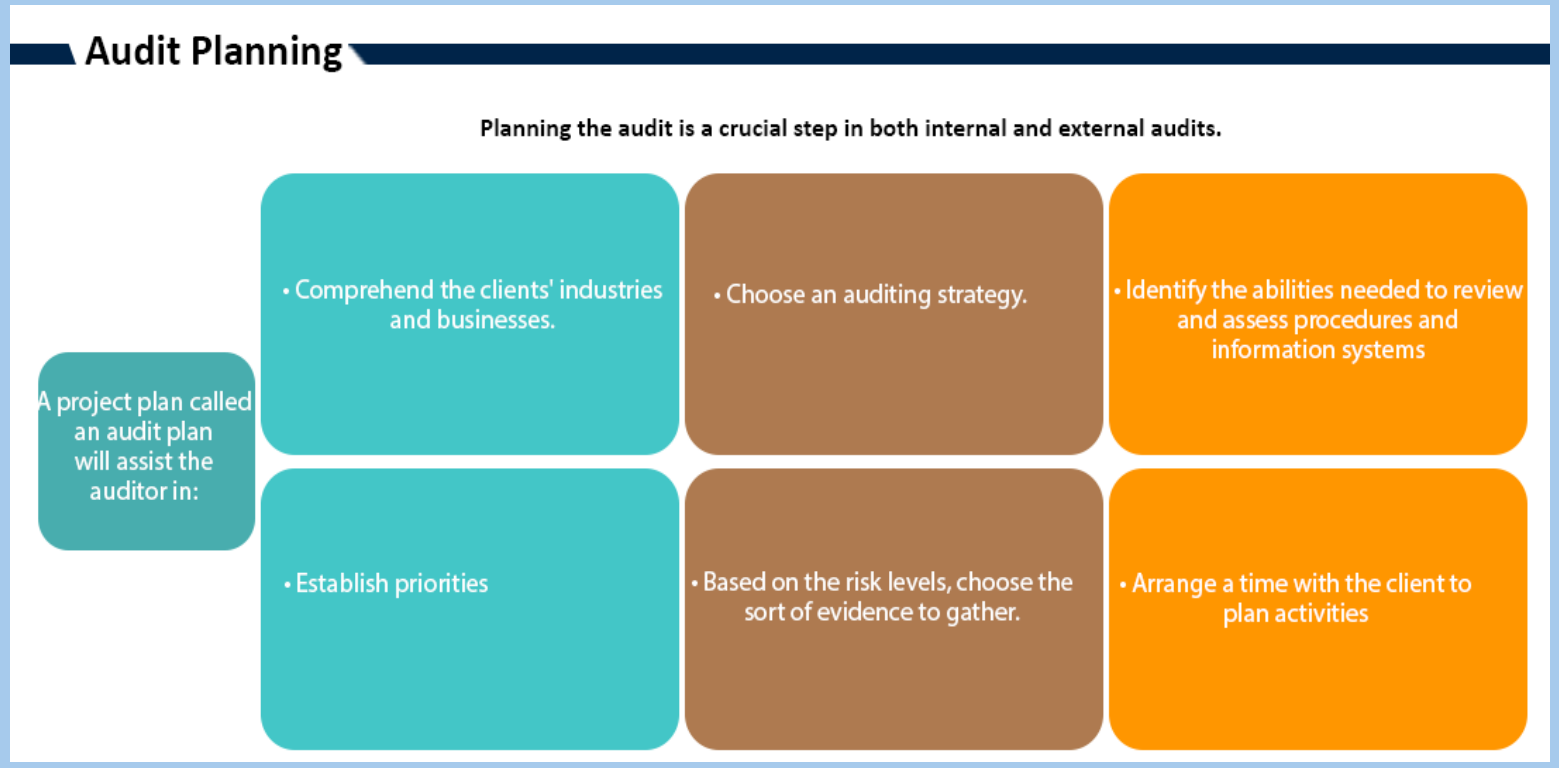
Steps to conduct Internal Audits

- Create Charter
- Assessment
- Reporting
- Remediation



Audit Strategies

- Goal (why audit conducting)
- Scope – determine boundaries
- Audit Team – Tools, resources, budget
- Plan
- Conduct - Review process, docs, VA, PT, facility visit
- Documentation



Third-Party Audit and Assessment

The security controls of the supply chains and service providers are assessed by independent third parties.

A particular clause for the right to audit must be included in the third-party contract with the contractor or vendor.

Supply chain security standards:

- ISO 28000
- UK NCSC (National Cyber Security Centre) Principles

Elements of Audit Findings

Condition – Results – if Controls present
Criteria
Cause
Effect
Recommendations

External audit also called Formal Assessment
Internal audit also called informal assessment

Remediation

The outcomes of the internal assessment may show areas that need improvement or remedial action.

- A timeframe for addressing the audit results should be established.
- Throughout the assessment, issues should be given a priority and remedied.
- Internal assessment needs to be improved upon continuously.

Plan of Action and Milestones (POAM) is a document that lists remediation tasks. It includes information on the resources needed to complete the plan's components, any task completion milestones, and scheduled completion dates for the milestones.

SOC REPORTS AND SECURITY ASSESSMENT

SOC REPORTS ARE DESIGNED TO HELP SERVICE ORGANIZATIONS, AND ORGANIZATIONS THAT OPERATE INFORMATION SYSTEMS AND PROVIDE INFORMATION SYSTEM SERVICES TO OTHER ENTITIES, BUILD CUSTOMER TRUST AND CONFIDENCE IN THEIR SERVICE DELIVERY PROCESSES AND CONTROLS THROUGH A REPORT BY AN INDEPENDENT CERTIFIED PUBLIC ACCOUNTANT (CPA)

SOC REPORTS ARE A SET OF ACCOUNTING STANDARDS THAT EVALUATE THE CONTROL OF FINANCIAL INFORMATION FOR A SERVICE ORGANIZATION.

SOC report is designed to help service organizations meet specific user needs for each of the following type:

SOC1 Report

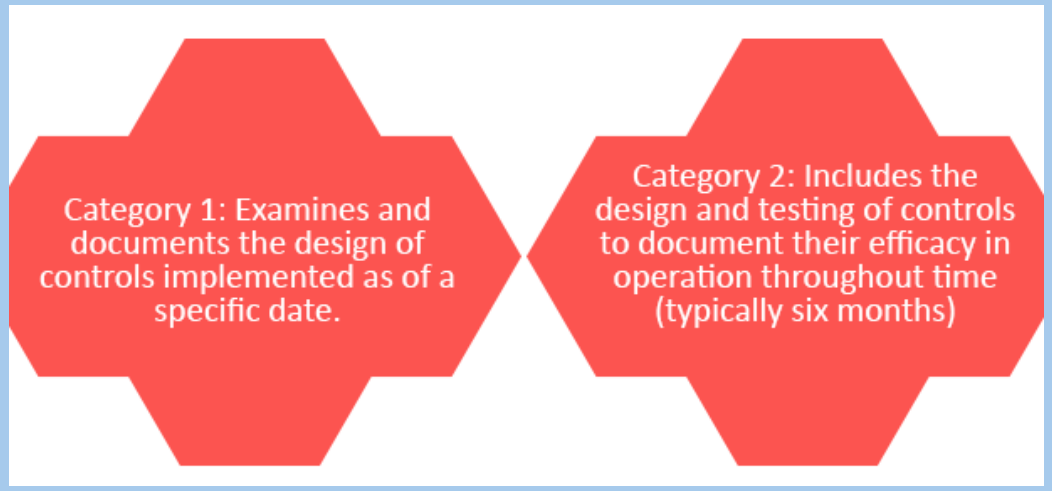
- Auditor covers financial & Security
- Capture on one time
- When audit conduct for short time (week on month)

Internal Controls over financial reporting

Auditors use this report

Type 1 – for single point of time

Type 2 – for six month time period



SOC2 Report

- When conduct Security audits
- Capture in 6 months
- When monitor Controls for 6 months and then generate report

Assess Controls for compliance and operations

Use for management

SOC3 Report

- High level Report and can show to 3rd party

Public facing report

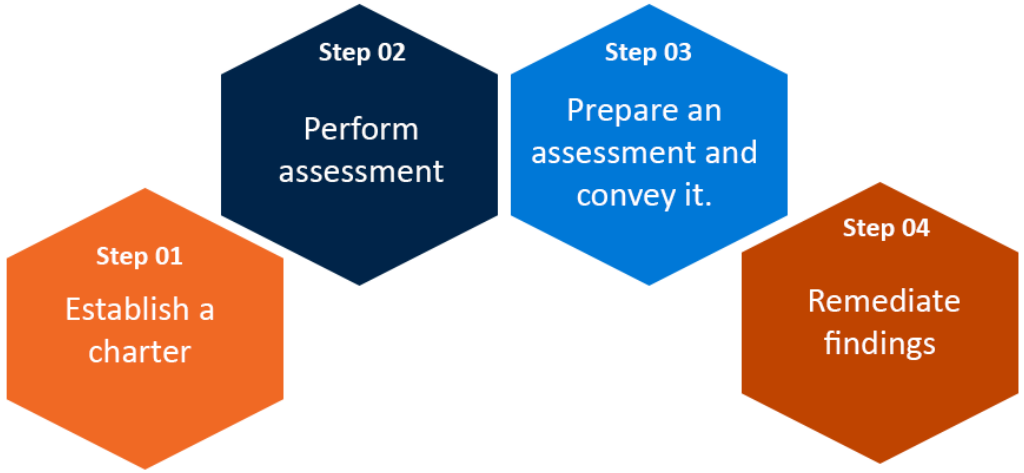
Security Assessment and Testing

- To identify the current level of security for the business or information system, security assessments are conducted.

Early detection of technological, operational, and system flaws is the aim of security evaluation and testing.

- By providing suggestions for improvem
enables the organisation to achieve a secu
risk and benefits the busi

Steps to Conduct Internal Assessment



Scope of Assessment

The assessment's scope will include the people, procedures, and technologies employed to support the business's physical, technical, and administrative controls. Following are the two kinds of assessments based on the scope.

Vulnerability assessment

The process of identifying vulnerabilities in IT and assessing the risks associated with those flaws is known as vulnerability assessment.

Penetration test

A penetration test evaluates a system's security by simulating an actual attacker trying to break into a target system.

In contrast to a vulnerability assessment, a penetration test not only identifies potential holes but also makes an attempt to attack them.

Vulnerability Assessment

- Weakness in a system, can be exploited by hackers
- Once Vulnerability found – report to SH
- Vulnerability related to people
- Vulnerability related to facility
- Vulnerability related to IT

Mis-configuration

Outdated software

Lack of patching

Tools: Nessus, OpenVAS

Types

- Technical Vulnerability
- People Vulnerability
- Physical Vulnerability

- When tester found Vulnerability -> then provide rating -> Create Report

Vulnerability Assessment

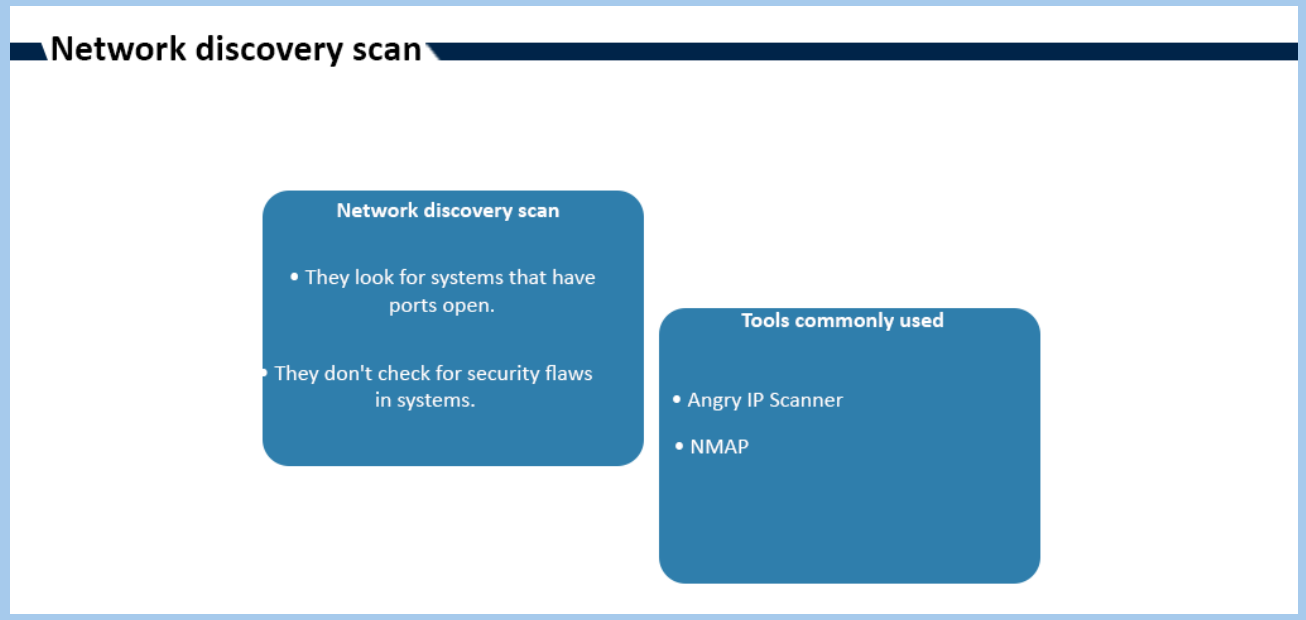
- Specify the resources or assets.
- Determine each resource's vulnerabilities or potential threats.
- Determine and put into action strategies to lessen the effects of a potential attack.
- Give the identified resources a measurable level of importance.
- Create a plan to reduce or eliminate the most significant vulnerabilities of the most important resources.

Types of Vulnerability Assessments

Personnel testing	• Demonstrating social engineering assaults and spotting holes in staff best practises.
Physical testing	• Examining facility and perimeter security measures • Carrying out vulnerability analyses for physical security
System and network testing	• Assessing the system using: o Network exploration scan o vulnerability analysis of a network o scanning for web application vulnerabilities

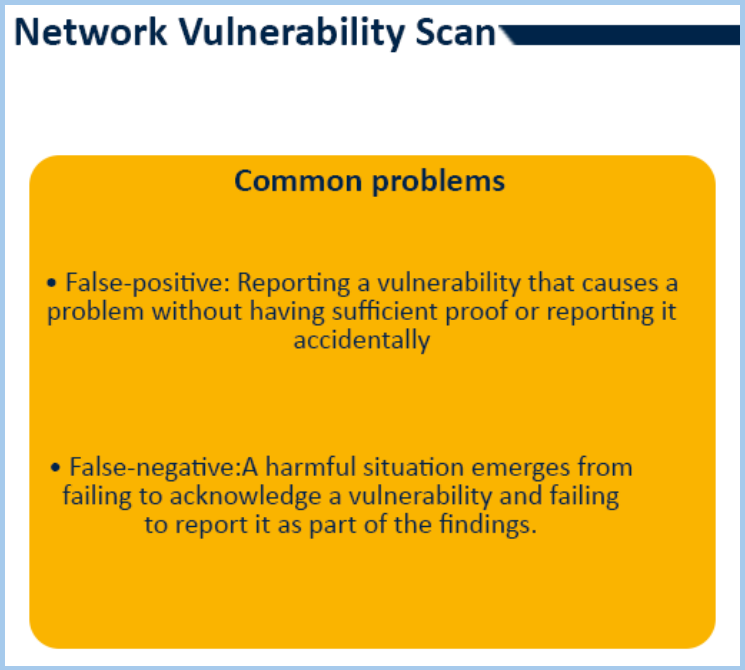
Technical Vulnerability Scan

- Planning
- Networking Discovery Scan
- Vulnerability Scanning
  - Network VS
  - Web VS
  - Data VS



❑ **Vulnerability Types**

- Physical – Related to people
- System testing – Technical Vulnerability
- Network testing – Technical Vulnerability



- **False Positive**
  - Reported vulnerabilities that doesn't exist
- **False Negative**
  - Vulnerabilities that not reported by tool – More dangerous
  - **Why false positive occurs**
    - If patches upgrades the file and old file was not removed. Tool scan the old file and find vulnerabilities
  - **Network Scanning Tools**
    - Nessus
    - OpenVAS
    - Microsoft Security Analyzer (MBSA)

Web Vulnerability Scan

- first-time application review of all submissions
- Examining any altered applications before they are put into use
- Checking any new applications before putting them into use
- The regular and scheduled scanning of all applications

Web Application Scan Tools BURPSuite

Web application scanners

QualysGuard, Burp Suite, and Acunetix

Penetration Testing

Identify vulnerabilities & exploit

Five steps

1. **Discovery** - Footprint and gather information about the target
2. **Enumeration** - Performing port scans and resource identification Methods
3. **Vulnerability Mapping -** Identifying vulnerabilities in identified systems and resources
4. **Exploitation -** Attempting to gain unauthorized access by exploiting vulnerabilities
5. **Report to Management -** Delivering to management documentation of test findings along with suggested countermeasures

- **Tools**
  - MetaSploit – Exploit the Vulnerability
  - KaliLinux

Red Team – Attacking Team

Blue Team – Defensive Team

Planning

- Identify the purpose
- Scope
- Types of Pen Testing
- Resources
- Written Authorization

Info Gathering

If doing black box testing – no info required
Go in public and find out name, email, contact etc.

Penetration Testing Types

Black box (zero knowledge) – External

- Pen test – No info, go to public spaces
- Public spaces – internet
- Also called Dynamic testing

Grey box (External)

Organization provides some info (IP)

White box (internal)

They have all organization info
Technology, systems, applications
Also called Static Code Review

Blind test

Organization contact pen testers for testing

Security Team knows what testers are doing

Double Blind Test

Organization contact pen testers for testing
Security Team doesn’t know about testing
In this way management can determine what Security Team done

Targeted testing

Focus testing

Logs Management & Review

- All the logs stored in central place
- In this way if hackers hack the one system so they cant delete the logs because logs are stored in central place

Procedures and guidelines used to control and facilitate the production, transmission, analysis, storage, archiving, and eventual disposal of the massive amounts of log data produced by an information system.

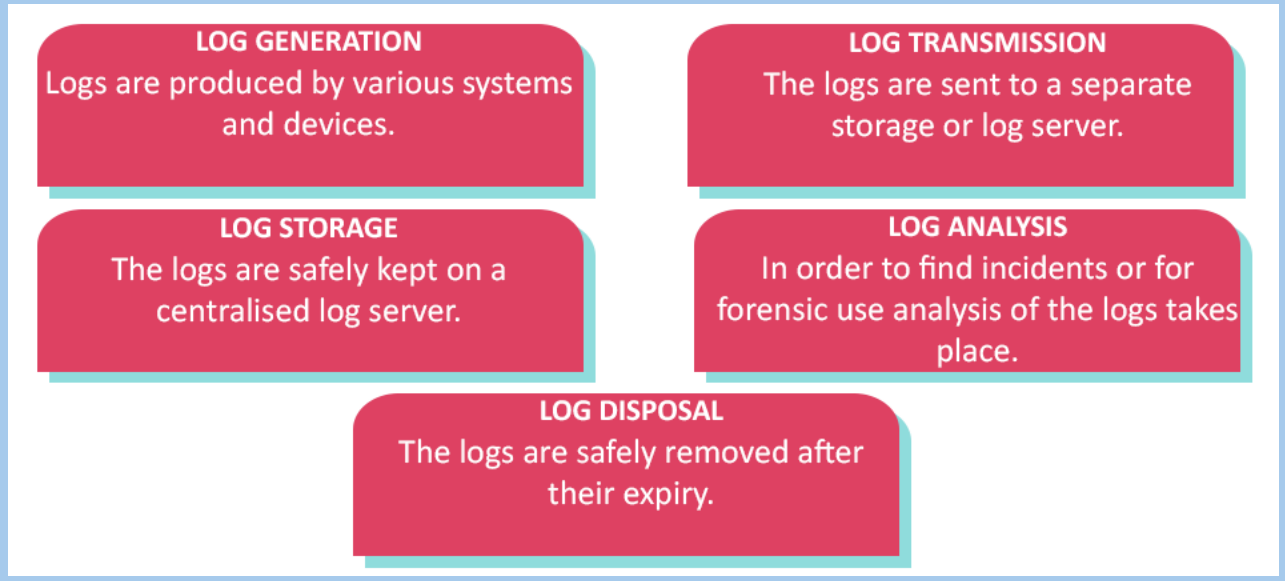
To identify security events or confirm the effectiveness of security measures, system logs are analysed.

The synchronisation of time across all log sources is a key requirement for an effective log review.

Logs are generated by a variety of sources, including firewalls, intrusion detection and prevention systems, antivirus software, and firewalls, in addition to documents pertaining to computer security.

Phases of Logs Management

- Logs Generation – Logs generated from end point
- Logs Storage – Store in central place
- Logs Analysis - SIEM
- Logs disposal



Logs Management - Advantages

- Investigation
- Audit
- Security Incident
- Operational issues

Challenges

- If time stamp not synchronized, then info is not reliable

Best Practice

- Define roles and responsibilities
- Identify relevant staff and provide Training
- Establish Policies

Security Testing in SDLC

Requirement Identification Phase

- Features
- Security issues
- Privacy issues

Design Phase

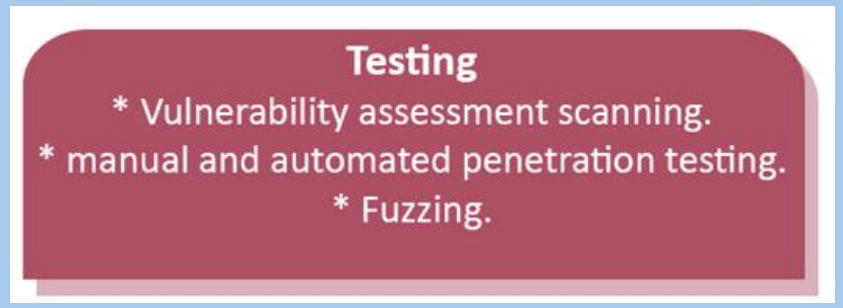
Identify Controls

Development Phase

Security testing done CODE REVIEW

Testing Phase

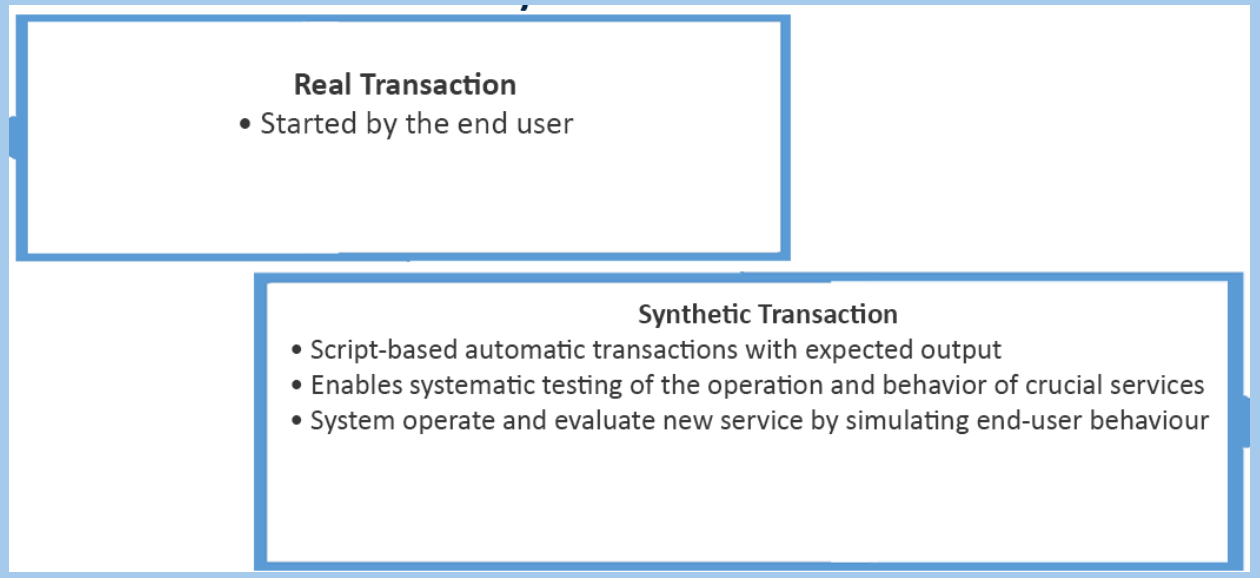
- Static
- Dynamic
- Unit
- Integration
- System
- Regression
- Fuzz
- User acceptance
- Threat Modeling
- Vulnerability test
- Penetration Testing



Application Testing

- **Real Transaction**
  - Testers manually provide some inputs to applications
  - This is REACTIVE
  - When issue happens then we know

- **Synthetic Transaction**
  - Use test cases (automated scripts)
  - This is PRO-ACTIVE
  - Can predict issue before happen



Types of Testing

- **Dynamic Testing**

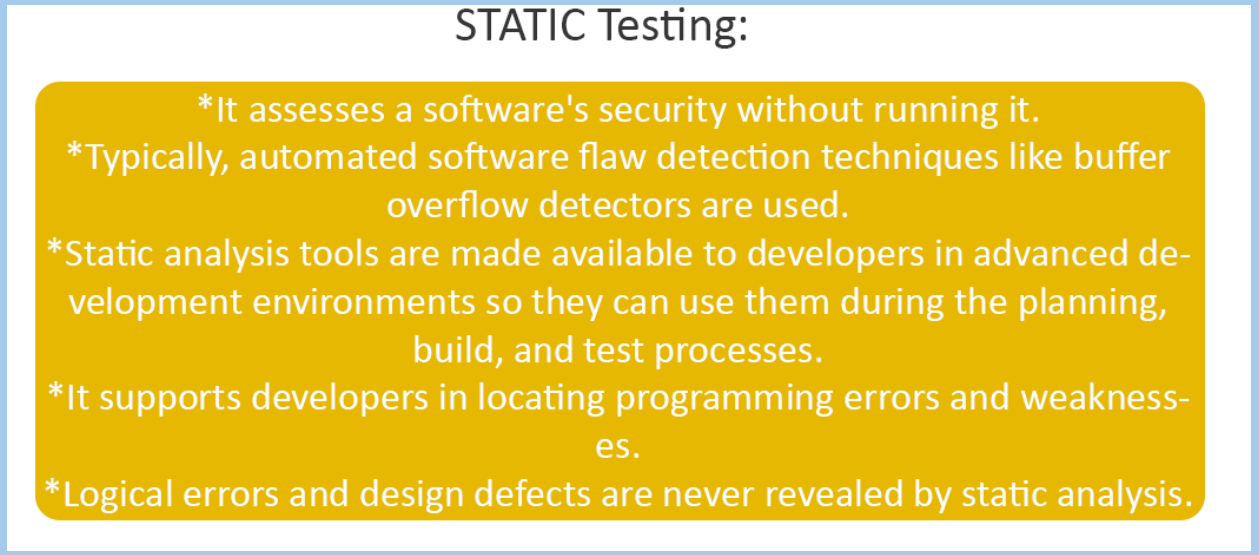
Active testing, when code is executing

Dynamic Testing:

*It assesses the security of software in a runtime environment and is frequently the only option for organisations that rely on others to deploy applications.
*Testers may not always have access to the source code.
*Synthetic testing can be used in dynamic testing.
*It can perform compatibility tests, detect memory leaks, identify dependencies, and analyse software without requiring access to the software's source code.

Static Testing

Require access source code
Also called white box testing



Passive testing, when code is not running

Source code review manually without running the code

Dynamic Testing

Mutation (Dumb) Fuzzing

Provide different Data type & length of inputs to see application behavior

Generational (Intelligent) Fuzzing

Data type fixed
Data length varies

Use Case Testing or Positive Testing

Check if required features are implemented
Provide valid inputs only

Misuse Case Testing

What are the possible Threats to identify
Provide invalid inputs only

Valid inputs – cell phone no/DoB

Grey box testing

Review some portion of code

UAT

Run the app and gibe access to end users

End user check if system is running

Unit Testing

To check if code of each module implemented

Test verify the functionality of software

White box testing

Verify interfaces b/w components

Integration testing – Dynamic Testing/Black box testing

Find defects once code change

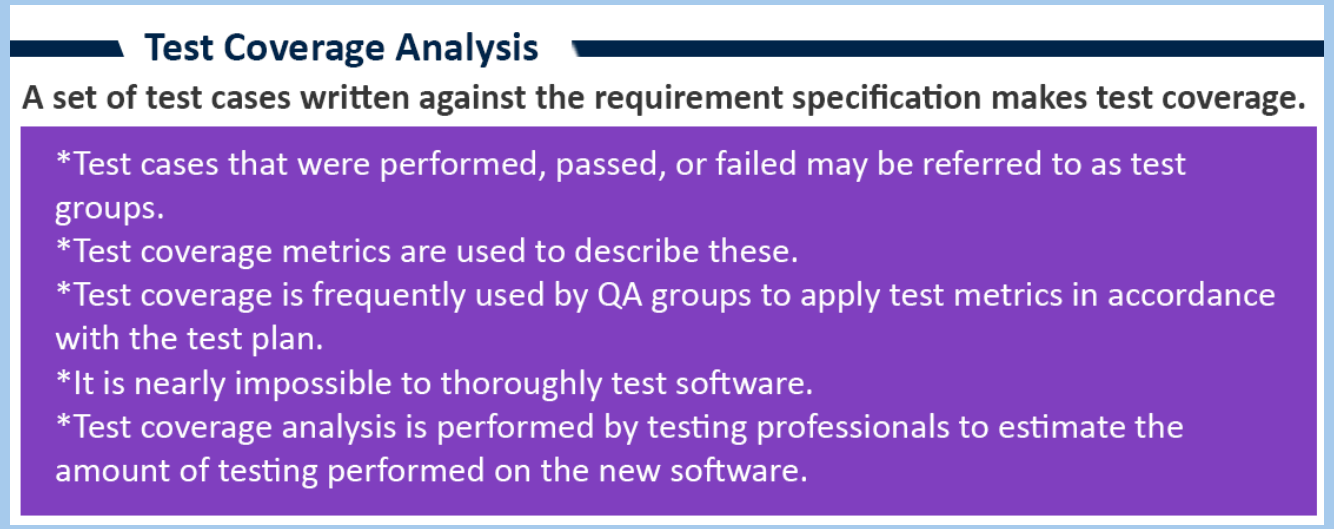
Regression Testing (Dynamic testing)

When make any changes in one module to see effect on another module

System Testing (Dynamic Testing)

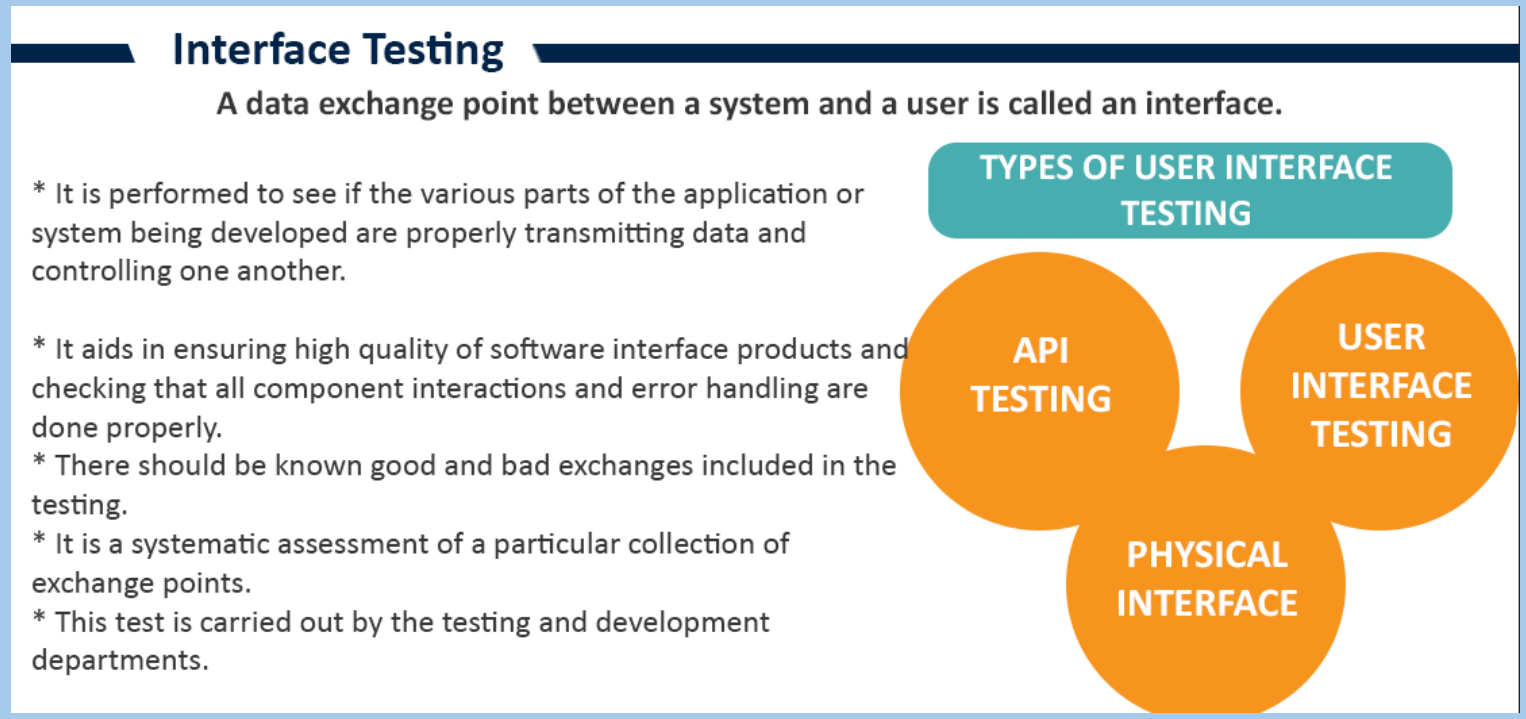
Test Coverage Analysis

- How much use case tested and completed, if 80 out of 100 features are tested so Test Coverage is 80%



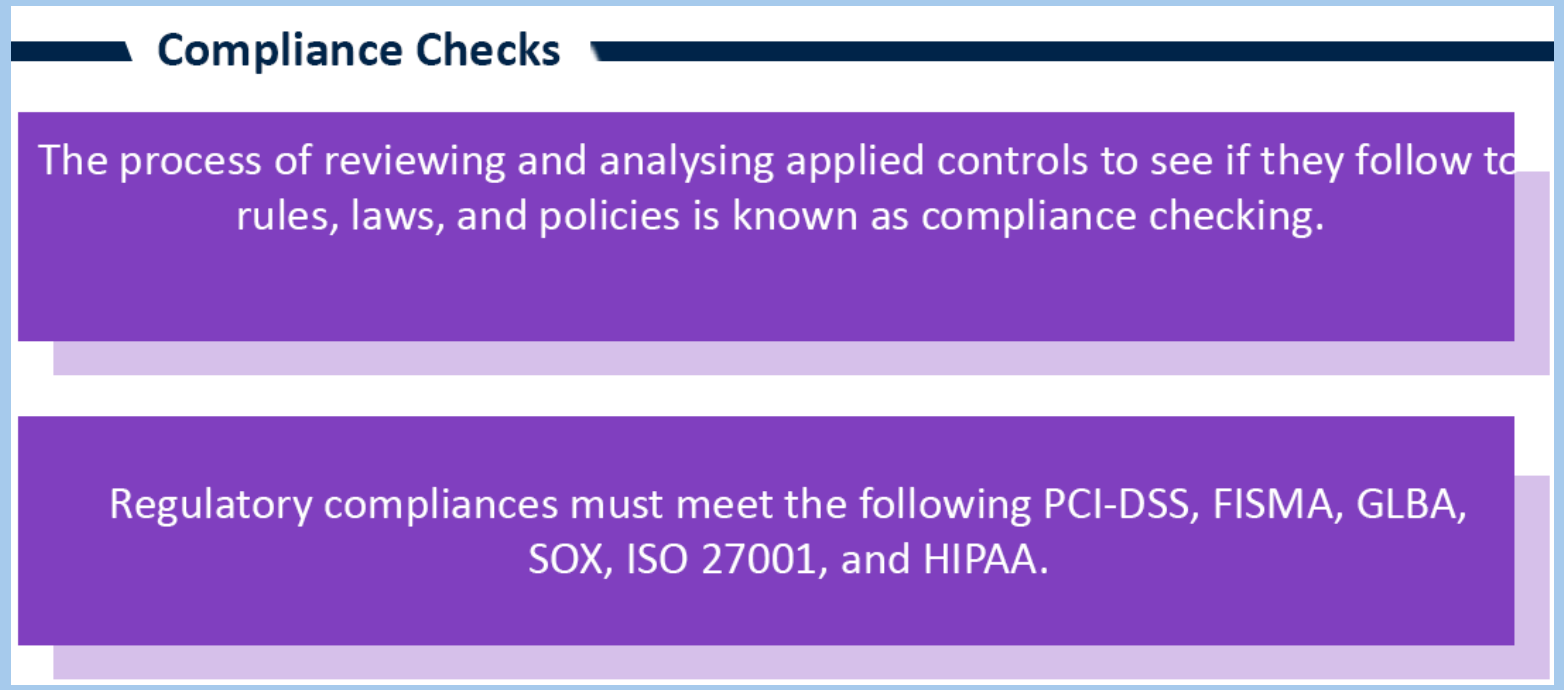
Interface Testing

App has multiple interfaces
User Interface – provide input from user interface



Compliance Test

- Test apps to make sure they are according to compliance standards
- ISO 27001, HIPPA, SOX, FISMA

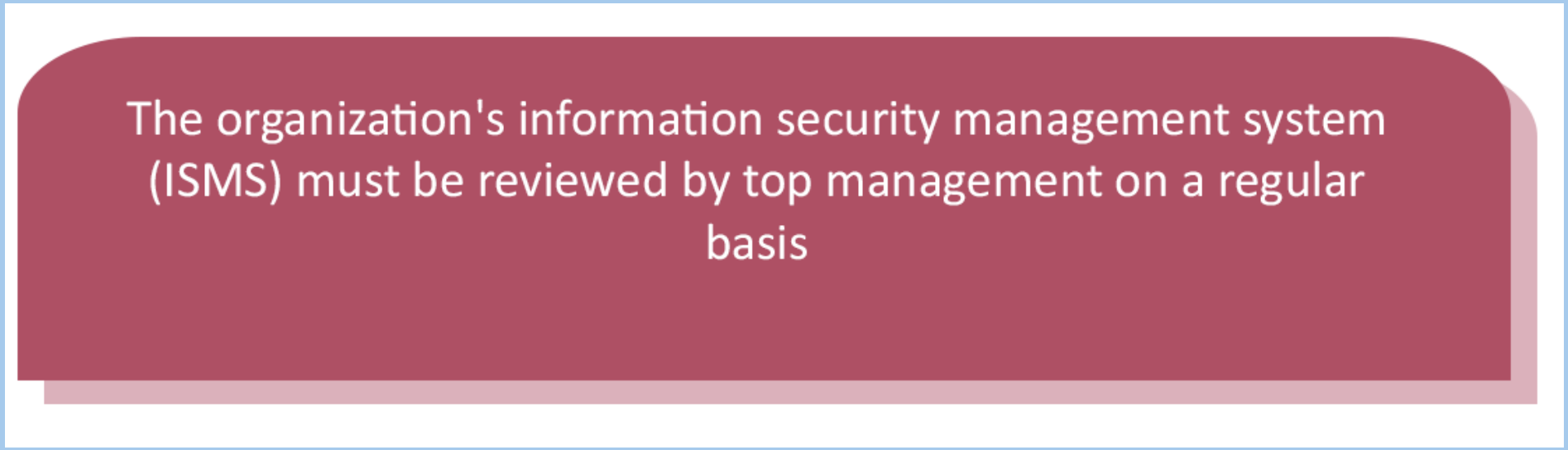


Management Review

- Audit
- Vulnerability Assessment
- Pen testing

- Technical reports sent to technical Team to review and take corrective action

- Executive reports sent to senior management to review and evaluate Controls that are according to requirements



KPI's – Technical Team Review

- To measure Controls or Risks
  - Tech Team
  - Security Team
  - CISO
  - Patches
  - Orphan accounts