Certified Information Systems Security Professional (CISSP) Certification Training Course

Domain 06: Security Assessment and Testing

Learning Objectives

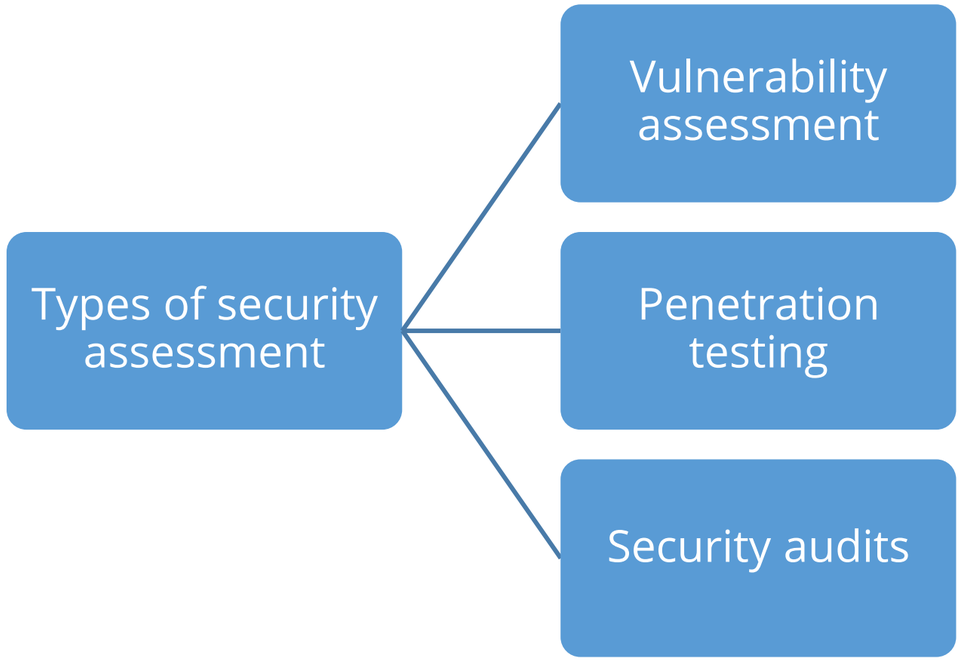
By the end of this lesson, you will be able to:

- Demonstrate assessment, test, and audit strategies
- Discuss penetration testing process and log management phases
- Examine different testing techniques and methods
- Discuss key performance Indicators and KPI process
- Compare different ethical disclosures

Introduction to Security Assessment and Testing

Security Assessment and Testing

- Security assessment is performed to identify the current security status of an information system or an organization.
- The goal of security assessment and testing is the early identification of technical, operational, and system deficiencies.
- The assessment provides recommendations for improvement which allows the organization to reach a security goal that mitigates risk and enables the organization.
- This is to ensure that appropriate and timely corrective actions can be applied before using the system in the production environment.



Design and Validate Assessment, Test, and Audit Strategies

Audits and Types of Audits

Audit

- An audit is a systematic, repeatable process, where a competent, independent professional evaluates one or more controls, interviews personnel, obtains and analyzes evidence, and develops a written opinion on the effectiveness of the control(s).
- The purpose of a risk audit is to provide reasonable assurance that adequate risk controls exist and are operationally effective.

Audits and Types of Audits

Internal Audit

- Performed by an organization's internal staff
- Reports are typically intended for an internal audience
- The disadvantage are:
  - Conflict of interest
  - Hidden agenda

External Audit

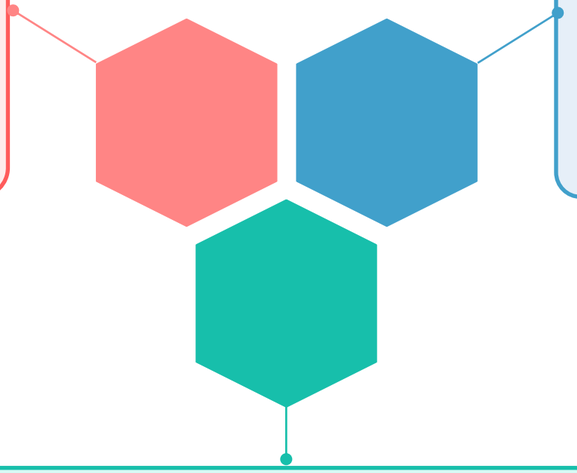
- Performed by third-party auditors
- Reports are intended for third-party stakeholders
- They are unaware of the internal dynamic and politics, hence they may not have any hidden agendas
- Major disadvantage is the cost
- Signing an NDA is a prerequisite

Internal and Third-Party Audits

Most regulations mandate an audit, which is an evidence gathering process.
There are three types of audits:

First-party

- Internal audit for and by the organization itself
- Used to confirm or improve the effectiveness of management systems



Second-party

External audit done by customers, regulators, or any external party with a formal interest in an organization

Third-party

External audit performed by independent organizations such as registrars (certification bodies) or regulators

Audit Strategy

Audit strategies:

- A clear set of goals should be established.
- The scope of the audit should be determined in coordination with business unit managers.
- The business unit managers should be included early in the audit planning process and should be engaged throughout the audit life cycle.

Audit can be driven by the following factors:

- Compliance requirements
- Significant changes to the architecture
- New developments in the threat the organization is facing

Audit Process

The audit process typically happens as described below:

01

Goal

Determine the goal of the audit

02

Involving stakeholders

- Bring in business unit managers at the earliest stage possible
- Ensure the business needs are identified and addressed

03

Scope

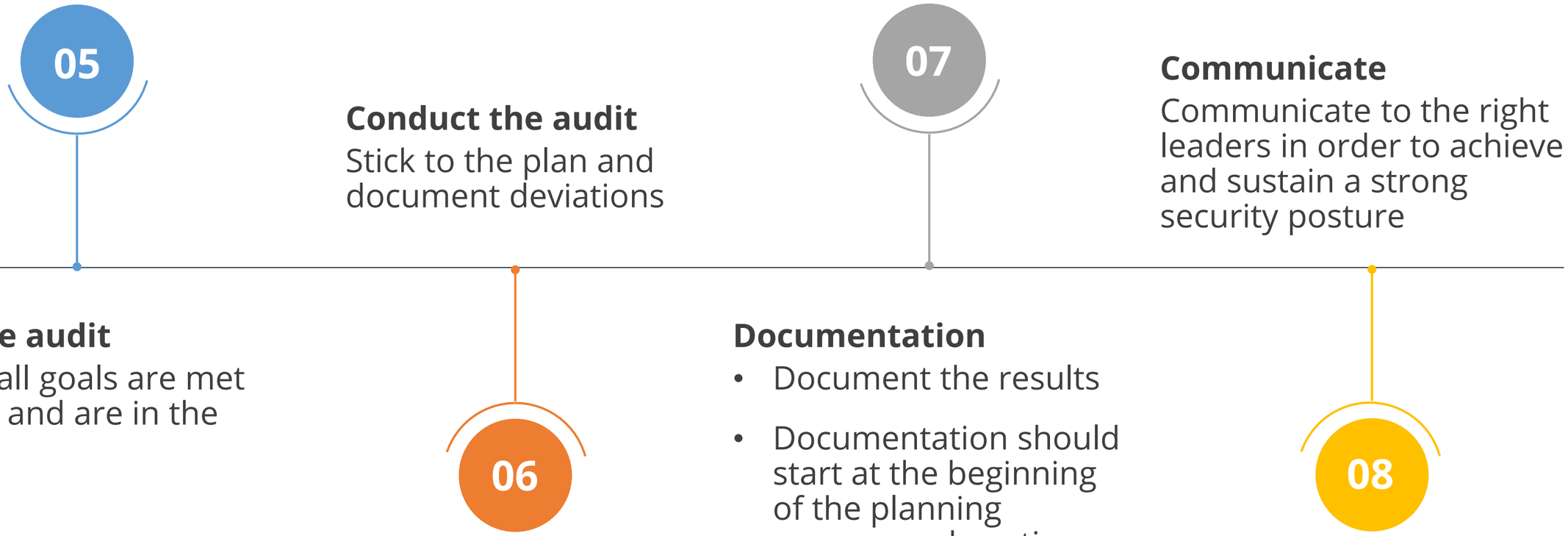
Determine the scope of the assessment

04

Audit team

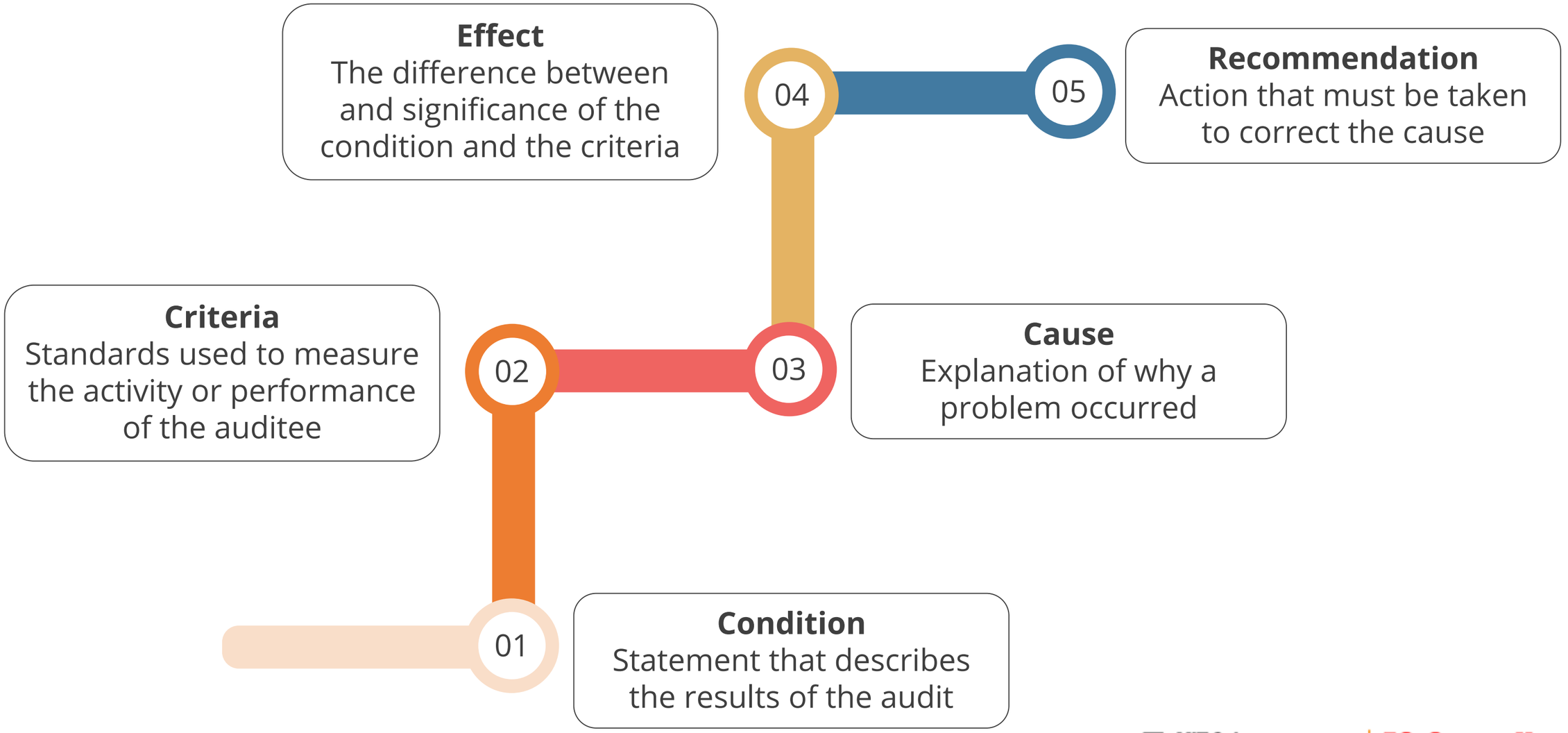
- Choose the right audit team
- Choose whether the team will consist of internal or external personnel depending on the goals, scope, budget, and available expertise

Audit Process



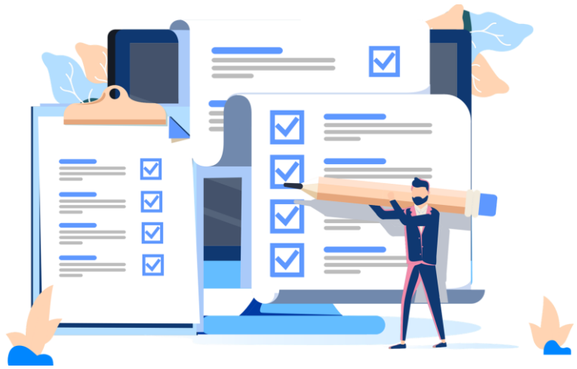
Elements of a Finding

The results of the audit have five elements in them, namely:



Assessments

An assessment is an evaluation of controls to meet management expectations.



Formal assessments are performed by **independent** assessors using procedures dictated by the relevant compliance standards.

The scope of the assessment is driven by compliance requirements such as GDPR, Sarbanes-Oxley Act or the Health Insurance Portability and Accountability Act (HIPAA).

The scope of the assessment and its reporting is determined by management.

Informal assessments might be performed by internal accessors and relies on documented and established organizational processes to improve controls effectiveness and efficiency.

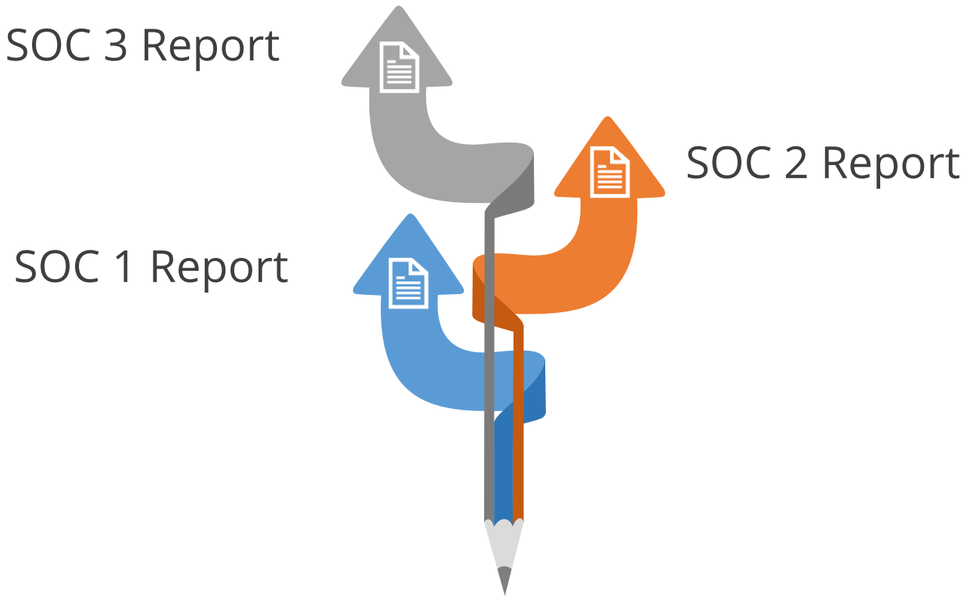
SOC Reports and Security Assessments

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 series of accounting standards that measure the control of financial information for a service organization.

SOC Reports and Security Assessments

Each of the following types of SOC report is designed to help service organizations meet specific user needs:



SOC 1 Report

The report on controls at a service organization relevant to user entities' internal control over financial reporting is prepared according to the Statement on Standards for Attestation Engagements (SSAE) 18 and is an enhancement to the previous standard for Reporting on Controls, the SAS 70.

There are two types of reports:

Type 1: Evaluates and reports on the design of controls put into operation on a certain date

Type 2: Includes the design and testing of controls to report on their operational effectiveness over a period (typically six months)

Use of these reports is restricted to the management of the service organization, user entities, and user auditors.

SOC 2 Report

This is a report on controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy. An SOC 2 report has the same options as the SSAE 16 report where a service organization can decide to go under a Type 1 or Type 2 audit. The criteria for these engagements are contained in the Trust Services Principles Criteria and Illustrations.

There are two types of reports:

Type 1: Report on management's description of a service organization's system and the suitability of the design of controls

Type 2: Report on management's description of a service organization's system and the suitability of the design and operating effectiveness of controls

Use of these reports is generally restricted and is at the discretion of the auditor using the guidance outlined in the standard.

SOC 2 Reports

SOC 2 is based on Trust Criteria modeled around four broad areas: Policies, Communications, Procedures, and Monitoring. The Principles and Criteria are jointly set by the AICPA and Canadian CPAs. The Trust Services Criteria are:

Security	The system is protected against unauthorized access, use, or modification, both physical and logical.
Availability	The system is available for operation and use as committed to or agreed upon.
Processing Integrity	System processing is complete, valid, accurate, timely, and authorized.
Confidentiality	Information designated as confidential is protected as committed to or agreed upon. It particularly applies to sensitive business information.
Privacy	The system's collection, use, retention, disclosure, and disposal of personal information meet commitments in any privacy notice and the GAPP.

SOC 3 Report

- Trust services report for service organizations is designed to meet the needs of users who require assurance about the controls at a service organization.
- These assurances affect the security, availability, and processing integrity of the systems used by a service organization to process users' information and the confidentiality or privacy of that information.
- SOC 2 report is useful to users who do not have the need for or the knowledge necessary to make effective use of an SOC 2 Report, but require the above mentioned assurances for control at an organization.
- SOC 3 reports can be freely distributed.

SOC 1, SOC 2, and SOC 3 Comparison

	PRUPOSE	INTENDED USERS	FOCUS ON	REPORT TYPE	EVALUATES
SOC 1	Audit of Financial Statements	Financial Statements Auditors, Customers, Related third parties	Internal controls relevant to Financial Reporting	Type I Type II	Design internal Control Operating effectiveness of internal Control during review period
SOC 2	GRC Programs, Oversight, Due diligence	Management, Regulators, Related third parties	Operational controls regarding security, availability, processing integrity, confidentiality or privacy	Type I Type II	Design internal Control Operating effectiveness of internal Control during review period
SOC 3	Marketing or General purpose	Anyone with a need for confidence in service organizations controls	Easy to read report on controls	General	Design of controls related to SOC2 objectives

Information source: https://accedere.io/soc-reporting-services.html

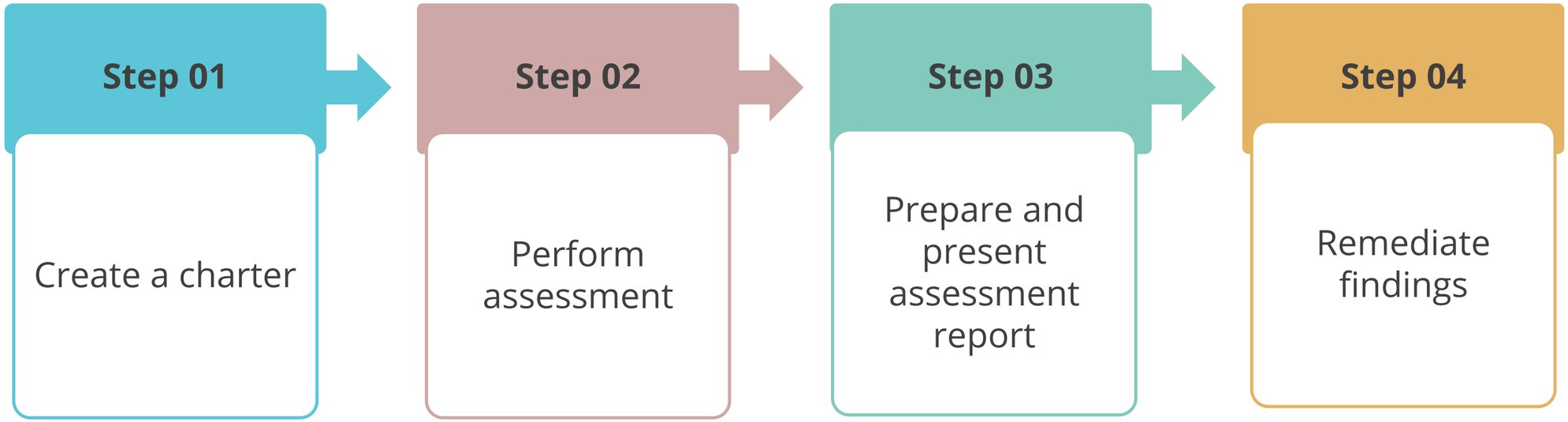
Internal Audit and Assessment

The purpose of internal assessment is to determine if the security controls meet the organization's risk expectations.

The internal assessment can help the organization to:

- Determine if the organization is meeting its own security standards
- Prepare for an external audit
- Increase staff awareness of security requirements
- Identify the gaps or areas for improving the efficiency of operations
- Understand where preventive or corrective action is needed
- Identify areas for security education or training needs

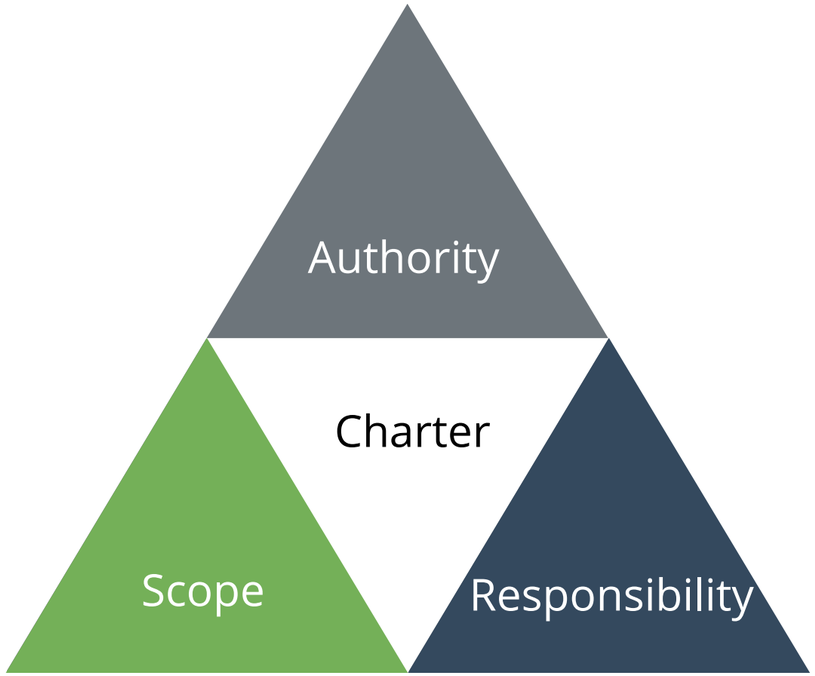
Steps to Conduct Internal Assessment



Charter

A **charter** is a formal document that defines the purpose, authority, scope, responsibility, and position of the people performing the assessment.

- The charter must be approved by the senior management.
- Scoping the assessment is also the responsibility of management.



Scope of Assessment

The scope of the assessment will address **physical**, **technical,** and **administrative** controls, including the **people**, **processes,** and **technologies** used to support the business. There are two kinds of assessments based on the scope:

Vulnerability assessment

- **Vulnerability assessment** is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated.

Penetration test

- **Penetration test** is the evaluation of system security in a realistic simulation of an attacker who intends to break into a target system.
- Unlike a vulnerability assessment, a penetration test not only identifies likely weaknesses, but tries to exploit the potential weakness.

Assessment Report

- The assessment report should document the process followed, observations, evidence, findings, conclusions, and recommendations.
- The assessment report should be presented to relevant levels of senior management.
- The exact format of the report will vary by organization.
- The levels of details presented will vary by various audiences.
- The report should contain sufficient evidence to support the findings.
- The audit artifacts collected during the assessment must be protected from alteration or inappropriate disclosure.

Remediation

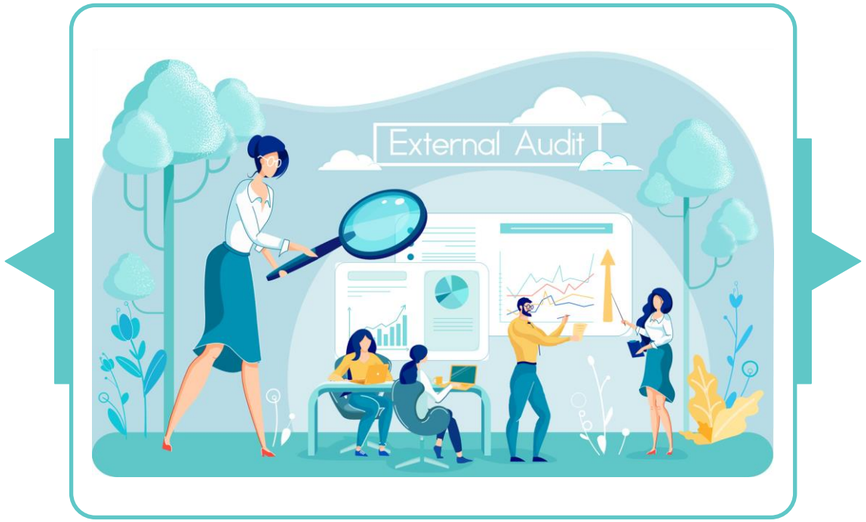
The results of internal assessment may identify areas where corrective actions or improvement is warranted.

- The timetable for remediation of the audit findings should be agreed upon.
- Issues identified should be prioritized and fixed during the assessment.
- Internal assessment should be subject to continual process improvement.

Plan of Action and Milestones (POAM) is a document that identifies tasks for remediation. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones.

External Audit and Assessment

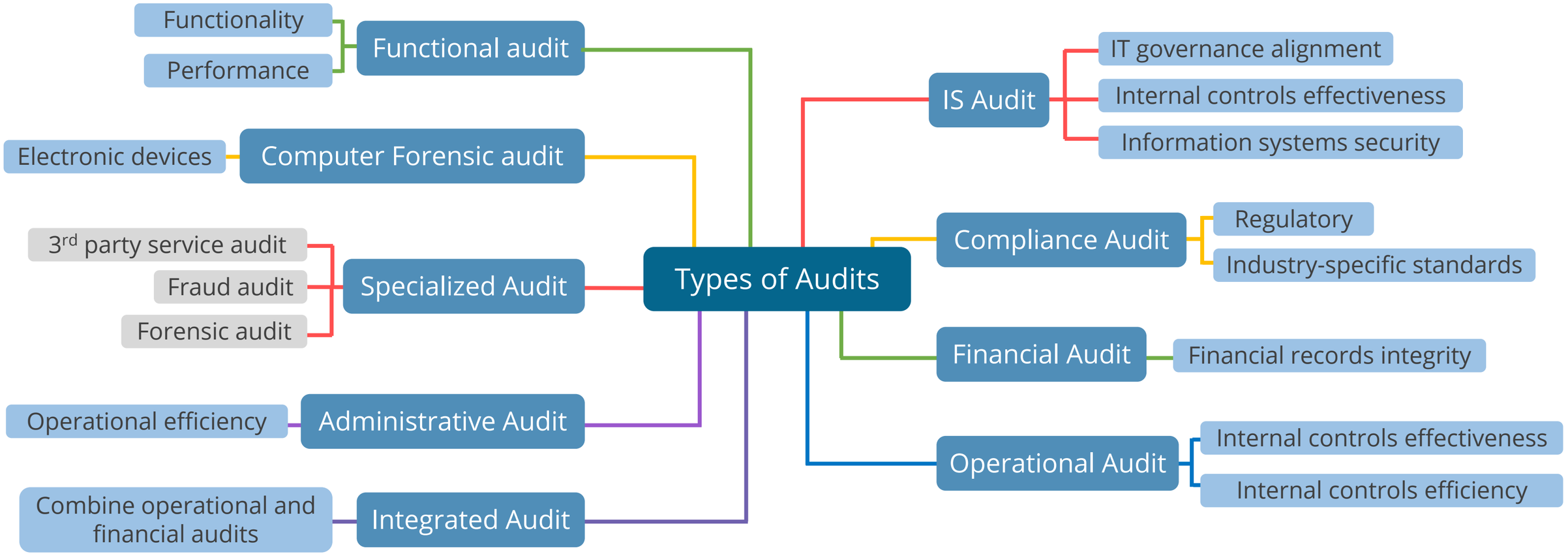
An audit is an assessment performed by an independent third-party to demonstrate that the organization's controls and practices meet a compliance standard.



Non-compliance could result in fines, litigations, limitations on business activities, or other consequences.

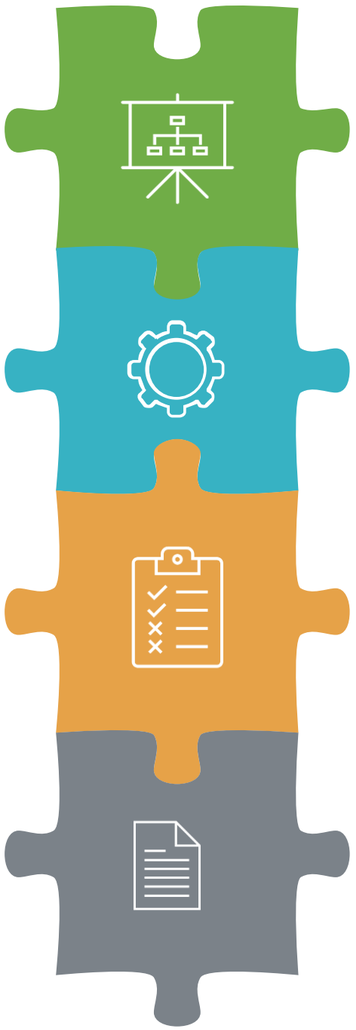
Types of Audits

The following diagram illustrates different types of audits.



Steps to Conduct an External Audit

Steps to conduct an external audit



- Create an audit charter
- Audit planning
- Perform audit
- Prepare and present audit report

Audit Planning

Audit planning is an important activity for both internal and external audits.

An audit plan is a project plan that will help the auditor to:

- Gain an understanding of the clients and their business
- Establish priorities
- Determine an audit strategy
- Determine the type of evidence to collect based on the risk levels
- Determine the skills required to examine and evaluate processes and information systems
- Schedule with the client to coordinate activities

Information source: https://www.schools.utah.gov/file/1e864d3a-9cd5-4933-a2f2-5d6e2a4e4535

Third-Party Audit and Assessment

Third-party audit and assessment evaluates the security controls of the supply chains and service providers.

The third-party contract with a contractor or vendor must contain a specific provision for the **right to audit**.

Supply chain security standards:

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

Principle of Supply Chain Security

There are four principles of supply chain security. They are explained below:

I. Understand the risks

- Understand what needs to be protected and why
- Know who your suppliers are and build an understanding of what their security looks like
- Understand the security risk posed by your supply chain

II. Establish control

- Communicate your view of security needs to your suppliers
- Set and communicate minimum security requirements for your suppliers
- Build security considerations into your contracting processes and require that your suppliers do this as well
- Meet your own security responsibilities as a supplier and consumer
- Raise awareness of security within your supply chain
- Provide support for security incidents

Information source: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

Principle of Supply Chain Security

There are four principles of supply chain security. They are explained below:

III. Check your arrangements

- Build assurance activities into your approach to managing your supply chain

IV. Continuous improvement

- Encourage the continuous improvement of security within your supply chain
- Build trust with suppliers

Information source: https://www.ncsc.gov.uk/collection/supply-chain-security/principles-supply-chain-security

Testing

Compliance testing (test of controls): Compliance testing determines whether controls follow management policies and procedures.

Substantive testing (test of details): Substantive testing evaluates the accuracy and integrity of individual transactions, data, or other information.

Presence of adequate internal controls (established through compliance testing) minimizes the number of substantive tests that must be done.

Conduct Security Control Testing

Vulnerability Assessment

Vulnerability

A vulnerability is defined in the ISO 27002 standard as ***a weakness of an asset or a group of assets that can be exploited by one or more threats*** (International Organization for Standardization, 2005).

Vulnerability assessment

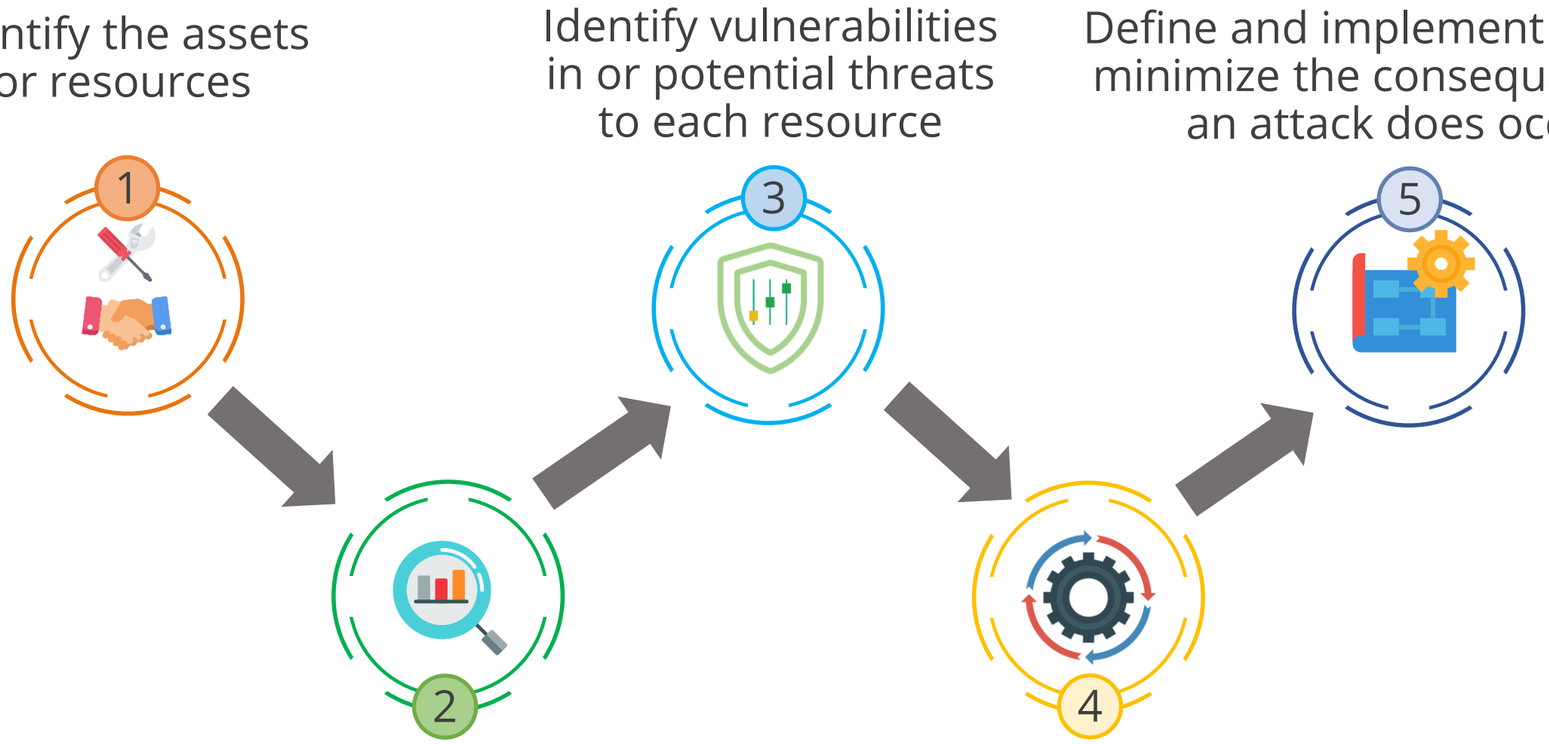
It is the process in which vulnerabilities in IT are identified and the risks of these vulnerabilities are evaluated.

Vulnerability assessment objectives

The main objective of a vulnerability management process is to detect and remediate vulnerabilities in a timely fashion.

Vulnerability Assessment

The vulnerability assessment steps are:



Types of Vulnerability Assessments

The three types of vulnerability assessments are:

Personnel testing

- Identifying vulnerabilities in standard employee practices and demonstrating social engineering attacks

Physical testing

- Reviewing facility and perimeter protection mechanisms
- Performing physical security vulnerability assessments

System and network testing

- Assessing the system using:
  - Network discovery scan
  - Network vulnerability assessment
  - Web application vulnerability scan

Network Discovery Scan

Network discovery scan

- They search for systems with open ports.
- They do not probe systems for vulnerabilities.

Tools commonly used

- NMAP
- Angry IP Scanner

Network Discovery Scan

There are four network discovery scan techniques:

TCP SYN scanning

- Sends a single packet to each scanned port with the SYN packet set
- If it receives a response with SYN and ACK flags set, this indicates the port is open at the sender's end
- This is also called half-open scanning

TCP connect scanning

- Opens a full connection to a remote system on the specified port
- Used when the user running the scan does not have necessary permissions to run a half-open scan

TCP ACK scanning

- Sends a packet with the ACK flag set, indicating that it is part of an open connection

Xmas scanning

- Sends a packet with the FIN, PSH, and URG flags set

Network Vulnerability Scan

Two common problems

- **False-positive**: Reporting a vulnerability without having substantial evidence to prove it or reporting by mistake, leading to a nuisance
- **False-negative**: Not identifying a vulnerability and failing to report it as a part of the results, leading to a dangerous situation

Network vulnerability scan

- It goes deeper than the discovery scan.
- It continues to probe the network for the presence of known vulnerabilities.
- The tools contain a database of known vulnerabilities along with the tests they can perform to identify these vulnerabilities.

Network Vulnerability Scan

Unauthenticated or noncredentialed scan:

- It is the process of exploring a network or a networked system for vulnerabilities that are accessible without logging in as an authorized user.
- It inspects the security of a target system from an outsider's perspective.

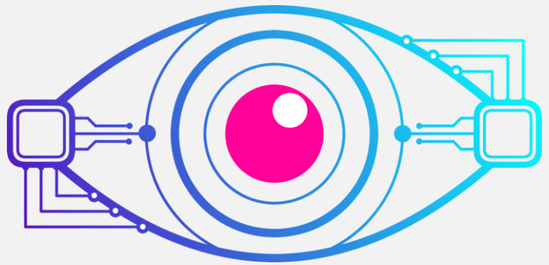
Authenticated or credentialed scan:

- It is a method in which vulnerability testing is performed as a logged in or authenticated user.
- Authenticated scans help reduce the false-positive or false-negative results.
- Authenticated scans are performed with read-only access to the servers being scanned.

Types of scans

Network Vulnerability Scan

- Tenable Nessus, OpenVAS, Microsoft Baseline Security Analyzer (MBSA), and Retina Network Scanner Community Edition



Tools used

Web Vulnerability Scan

Web vulnerability scan

- The process of testing, analyzing, and reporting on the security level and posture of a Web application
- Uses special purpose scanners that analyze Web applications for known vulnerabilities
- Can discover vulnerabilities not visible to network vulnerability scanners

Web Vulnerability Scan

Ideal scenarios

- Scanning all applications for the first time
- Scanning any new application before moving to production
- Scanning any modified application before it moves to production
- Scanning all applications on a scheduled and recurring basis

Web Vulnerability Scan: Tools

Web application scanners

- Acunetix, QualysGuard, and Burp Suite

Penetration Testing

- Penetration testing, also called pen testing or ethical hacking, is the practice of testing a computer system, network, or Web application to find security vulnerabilities that an attacker could exploit.
- Penetration testing is the process of determining the true nature and impact of a given vulnerability by exploiting existing vulnerabilities.
- Considered to be the next level in vulnerability assessments, it simulates an actual attack and is also known as ethical hacking, red teaming, tiger teaming, or vulnerability testing.
- Its goal is to measure an organization's level of resistance to an attack and to uncover any weaknesses within the environment.

Penetration testing:

Penetration Testing: Tools

- Metasploit, Kali Linux, and Aircrack-ng

Penetration testing tools:

Discussion

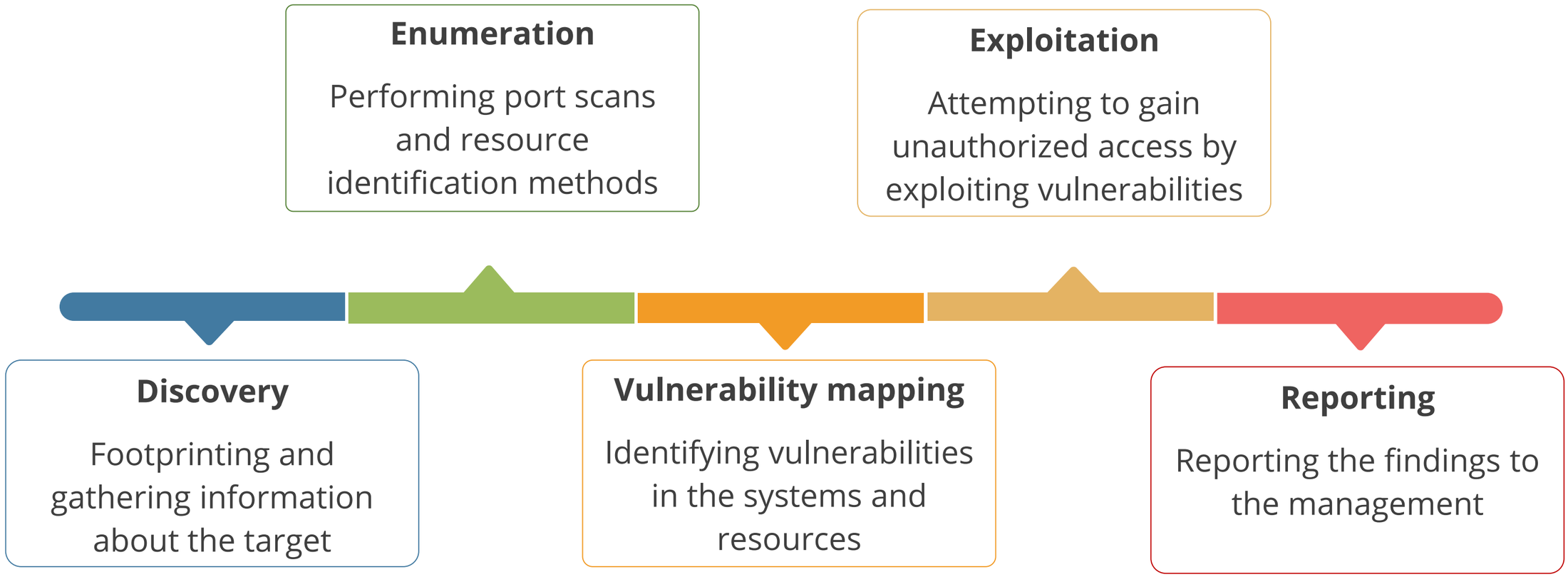
Discussion

A penetration test is considered a realistic emulation of an attacker who intends to break into the target system.

1. What could the organization do to ensure that the penetration tester does not disclose the sensitive or proprietary data during the test in an unauthorized manner?
2. What could the tester do to protect themselves from the legal implications of penetration testing which is technically similar to a real attack?

Penetration Testing Process

Phases of penetration testing:



Penetration or Vulnerability Testing Types

- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- Gray-box testing (partial knowledge)
- Blind tests
- Double blind types
- Targeted

- The tester has no prior knowledge of the internal design or features of the system.
- It is the most accurate method to simulate an external attacker.
- It will probably not detect all vulnerabilities.
- The testing team may inadvertently impact another system.

Penetration or Vulnerability Testing Types

- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- Gray-box testing (partial knowledge)
- Blind tests
- Double blind types
- Targeted

- The tester has complete knowledge of the internal system.
- It allows the test team to target specific internal controls and features.
- It may yield a more complete result.
- It may not be representative of an external hacker.

Penetration or Vulnerability Testing Types

- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- **Gray-box testing (partial knowledge)**
- Blind tests
- Double blind types
- Targeted

- Some information about internal working is given to the tester.
- It helps guide their tactics toward areas that need to be thoroughly tested.
- This approach mitigates the risks of the other two models.

Penetration or Vulnerability Testing Types

- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- Gray-box testing (partial knowledge)
- **Blind tests**
- Double blind types
- Targeted

- The tester only has publicly available data to work with.
- The network security team has prior knowledge of this test to defend against an attack.

Penetration or Vulnerability Testing Types

- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- Gray-box testing (partial knowledge)
- Blind tests
- **Double blind types**
- Targeted

- It is also known as stealth assessment.
- It is a blind test to both the tester as well as the security team.
- It is used to evaluate the security levels and responses of the security team.
- It is a realistic demonstration of the likely success or failure of an attack.

Penetration or Vulnerability Testing Types

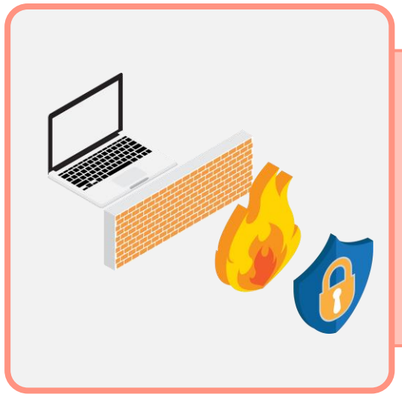
- Black-box testing (zero knowledge)
- White-box testing (full knowledge)
- Gray-box testing (partial knowledge)
- Blind tests
- Double blind types
- Targeted

- It involves external and internal parties carrying out a focused test on specific areas of interest.

Log Management and Review

In IT, an event log is a basic resource that helps provide information about network traffic, system traffic, and other conditions.

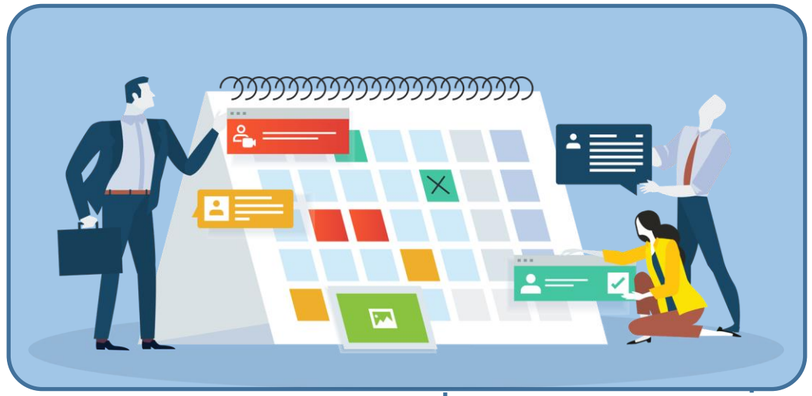
An event log stores these data for retrieval by security professionals or automated security systems to help IT administrators manage various aspects such as security, performance, and transparency.



Apart from records related to computer security, logs are generated from many other sources such as antivirus software, firewalls, intrusion detection, and prevention systems.

Log Management and Review

Log management is the collective processes and policies used to administer and facilitate the generation, transmission, analysis, storage, archiving, and ultimate disposal of the large volumes of log data created within an information system.



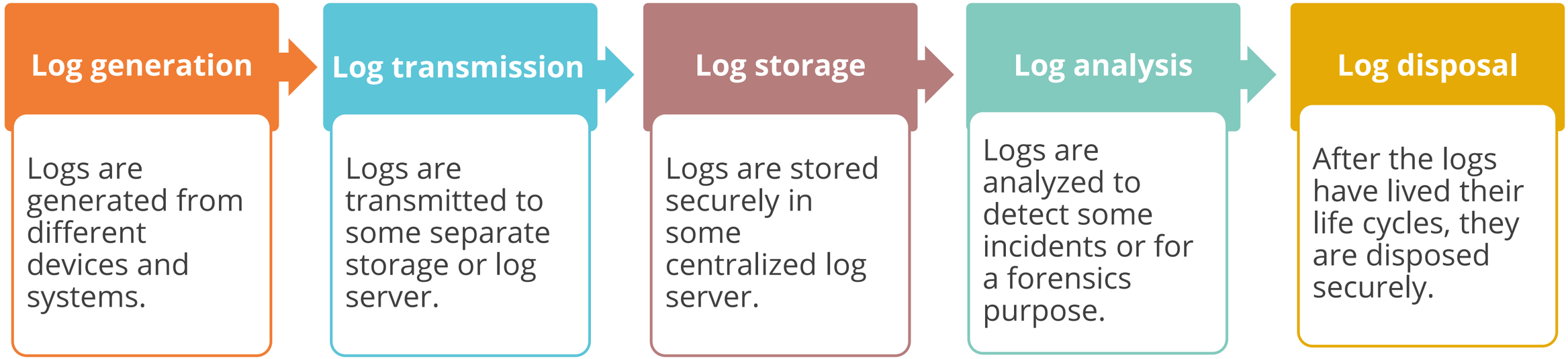
System logs are examined to detect security events or verify effectiveness of security controls.

Key requirement for an effective log review is the time synchronization across all the log sources.

NTP is the protocol for time synchronization (UDP 123).

Log Management Phases

Log management is done in the following steps:



Log Tampering Prevention

It is vital to maintain the integrity of log data. Here are the methods to prevent it from being tampered:

Remote Logging	Putting a log file into another device will protect it from being tampered with in a compromised system
Simplex Communication	• Using a one-way communication between the reporting devices and the central log repository • Accomplished by severing the **receive** pairs on an ethernet cable
Replication	Making multiple copies and keeping them in different locations
Write-Once Media	Using write-once media to prevent unauthorized modifications to log files
Cryptographic Hash	Powerful technique for ensuring unauthorized modifications are easily noticed

Log Management: Advantages and Challenges

Advantages

- Confidentiality, integrity, and availability of logs
- Forensic investigations
- Auditing
- Identifying security incidents
- Identifying fraud
- Identifying operational issues
- Establishing baselines

Challenges

- Managing large quantities of logs from various sources
- Discrepancies in log content, timestamps, and formats

Log Management: Best Practices

The best practices for log management are:

- Establish log management policies and procedures
- Prioritize requirements for log management process
- Define roles and responsibilities
- Create and maintain log management infrastructure
- Support the staff responsible for log management

Real Transaction and Synthetic Transaction

Real Transaction

- Transactions that are initiated by an end-user are called real transactions.

Synthetic Transaction

- Automatic script-based transaction with an expected output is called a synthetic transaction.
- It allows to systematically test the behavior and performance of critical services.
- It can help test a new service mimicking end-user behavior to ensure the systems work as they should.
- This is an effective way of testing the software from outside.

Real User Monitoring vs. Synthetic Transactions

Real User Monitoring (RUM)

- RUM is a passive monitoring technology which determines if users are being served correctly and quickly.
- It records all user interaction with a website or client interaction with a cloud-based application or server.
- It accurately captures the actual user experience.
- It tends to produce noisy data and thus may require more back-end analysis.
- It lacks the elements of predictability and regularity, which could mean that a problem won't be detected during low utilization periods.

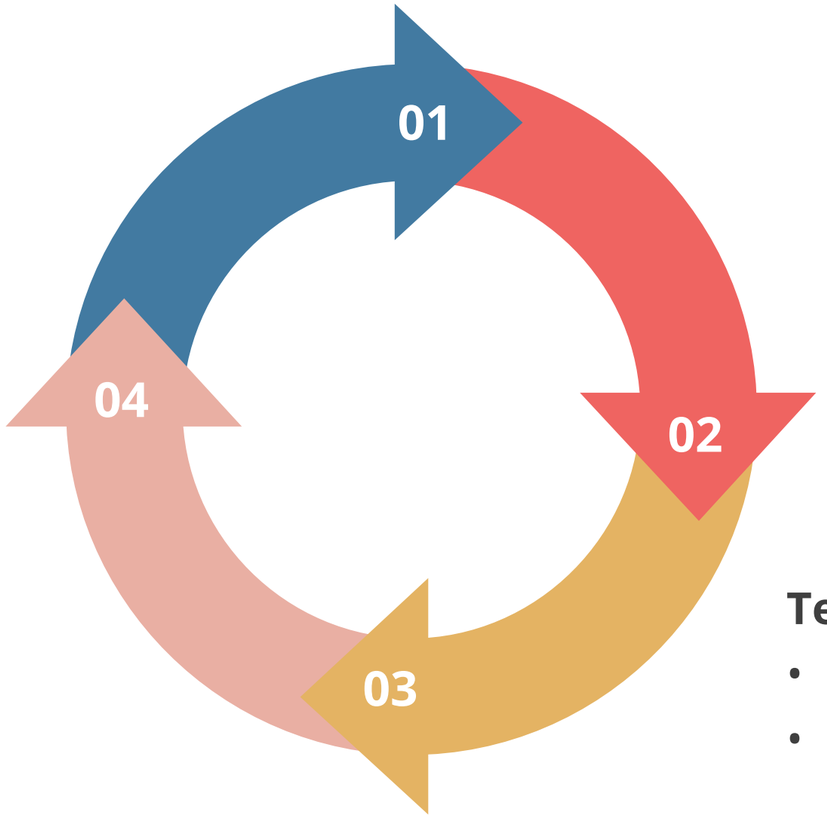
Synthetic Transaction

- Actions performed on monitored objects in real time are called synthetic transactions.
- Synthetic performance monitoring is proactive and involves external agents running scripted transactions against a web application.
- In synthetic transactions, real user sessions are not tracked.
- Some of the tools used are Microsoft System Center Operations Manager, Foglight Transaction Recorder.
- Some examples of functionalities are monitor websites, databases, and TCP ports.

Security Testing in the SDLC

Plan and Design

- Architecture security review
- Threat modeling



Application Development

- Manual code review
- Static Source Code Analysis
- Manual binary review
- Static binary review analysis

Operations and Maintenance

- Security testing of patches
- White box testing or code-based testing
- Black box testing

Testing

- Vulnerability assessment scanning
- Manual and automated penetration testing
- Fuzzing

Testing Techniques

Testing can be:

Manual		Automatic
Black box	AND	White box
Static		Dynamic

Conducting a test requires understanding of:

- Type of application
- Attack surface
- Technologies supported
- Quality of results and usability
- Performance
- Resource utilization

Software Product Testing Levels

The different levels of product testing are:

Unit level

- Tests individual units or components of a software or system
- Helps validate that each unit of the software performs as designed

Integration level

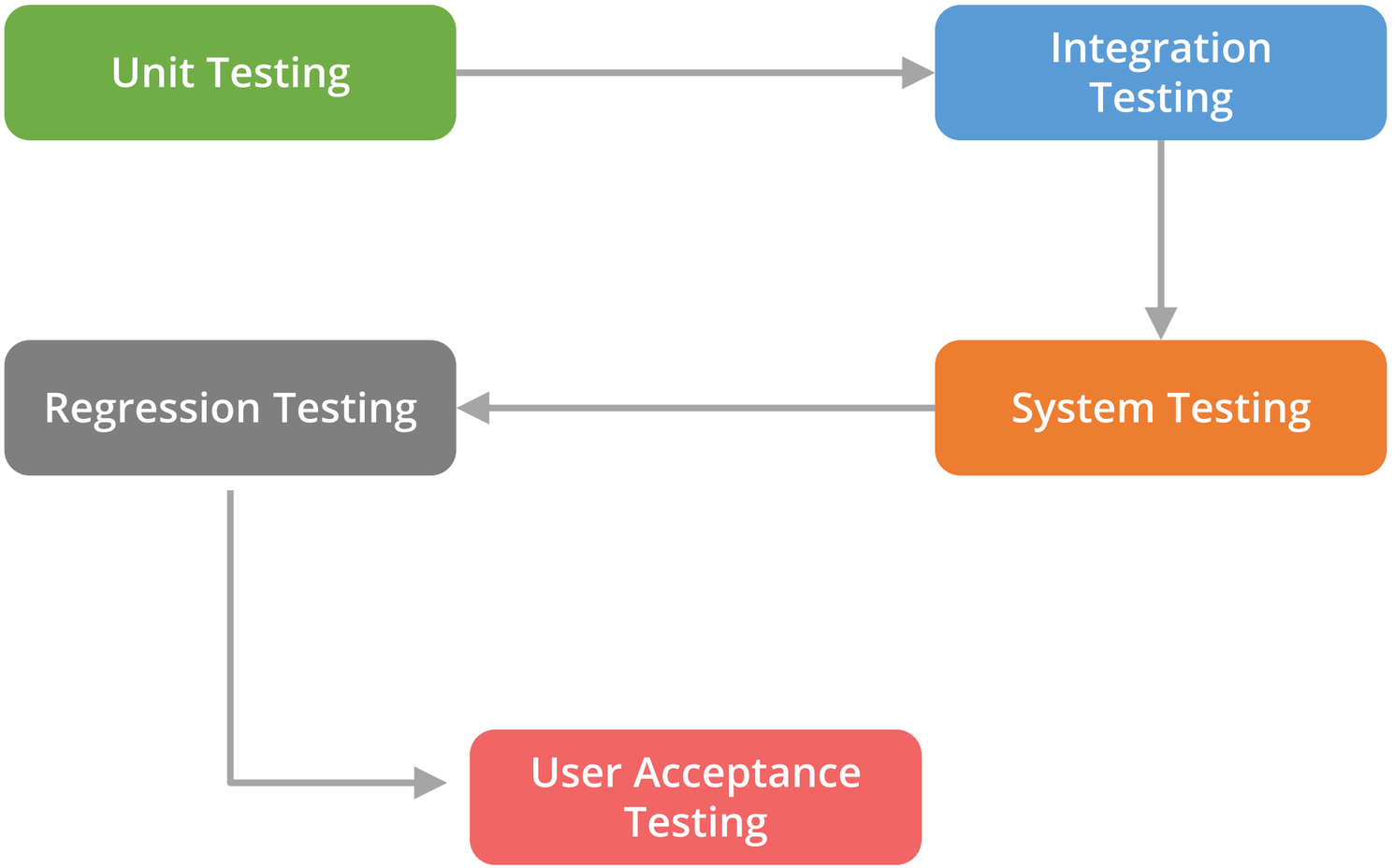
- Combines individual units and tests them as a group
- Helps expose faults in the interaction between integrated units

System level

- Tests complete, integrated system, or software
- Helps evaluate the system's compliance with the specified requirements

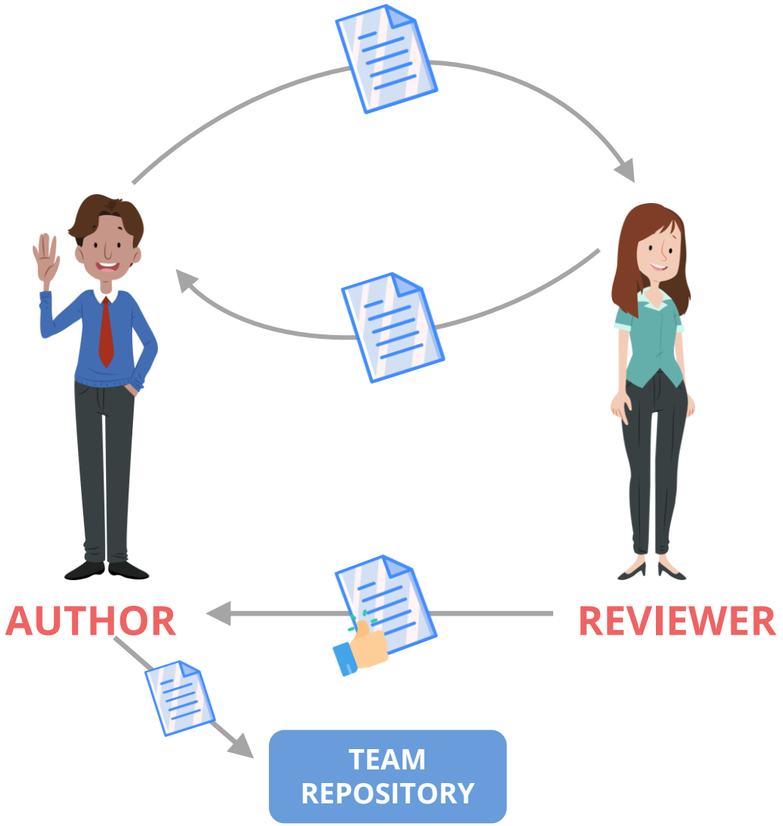
Software Testing Levels

There are five software testing levels. They are:



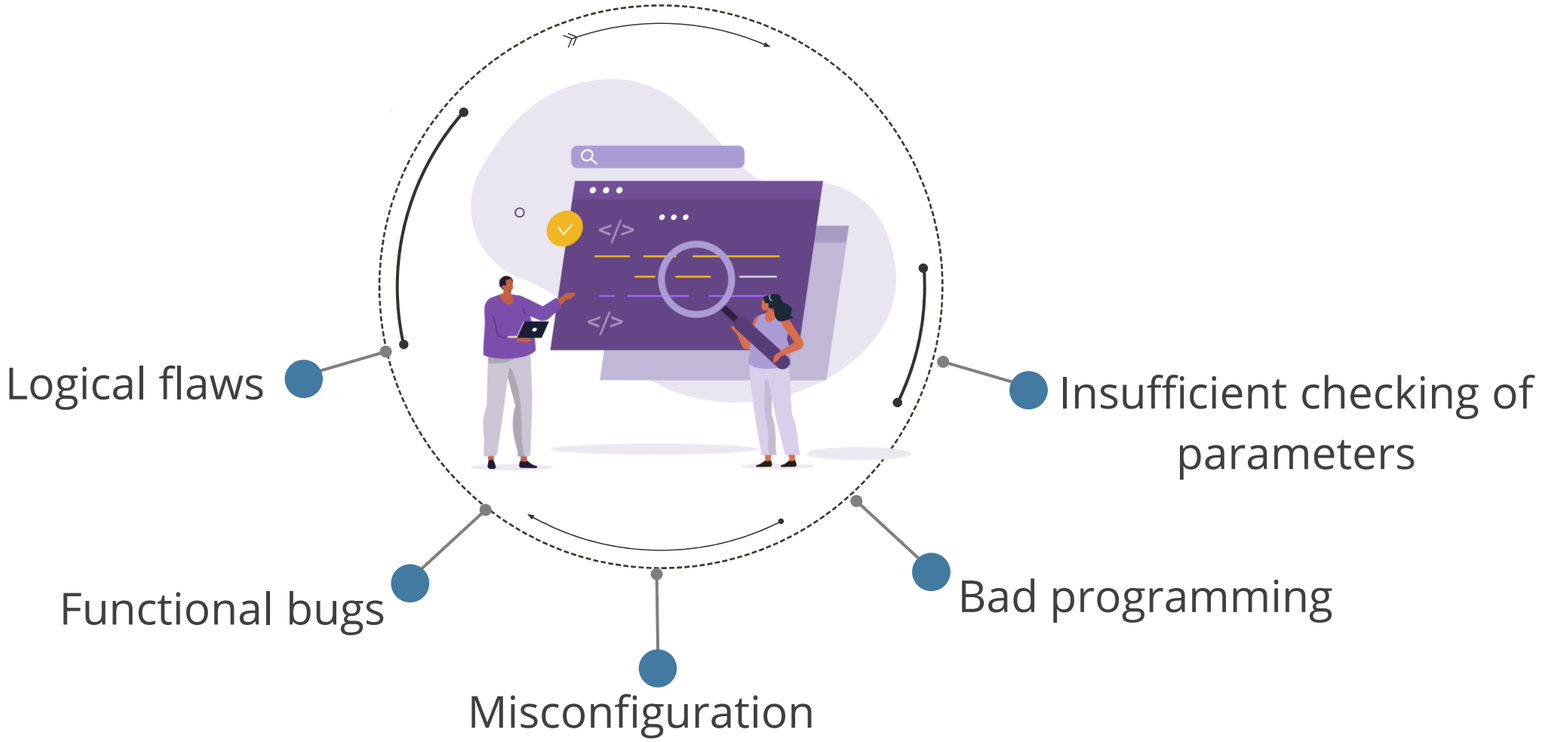
Code Review and Testing

- Code review is a systematic examination of instructions that comprise a piece of software performed by someone other than the author of that code.
- It is the foundation of software assessment programs.
- It is often known as peer reviews.
- It starts with the organization setting the coding standards to be followed.
- The preliminary step to code review is to ensure the developer followed the defined coding standard.
- After this step, the reviewer will check for functions which are not needed or procedures that may lead to a code bloat which makes it harder to maintain and secure the application.
- A coding error can make a system vulnerable and compromise its security entirely. Security must be included in all the phases of the Software Development Life Cycle (SDLC).



Code Review and Testing

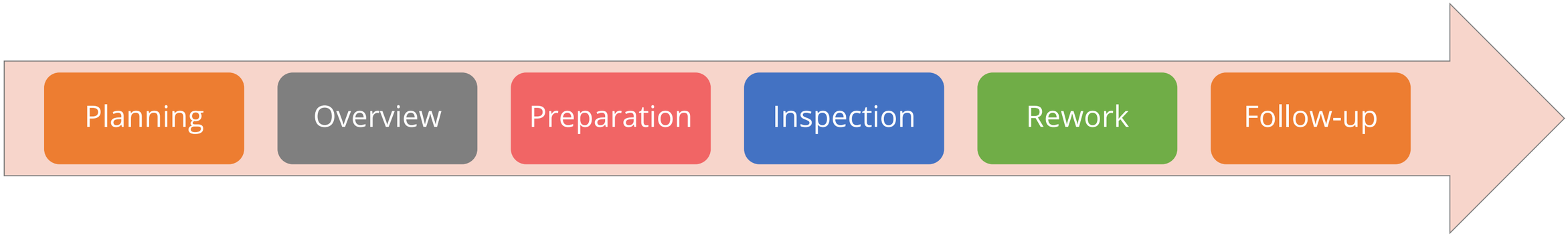
Software vulnerabilities are mainly caused by:



Fagan Code Review Process

- Fagan inspection is a process of trying to find defects in documents such as the source code or formal specifications during various phases of the software development process.
- It is named after Michael Fagan who is credited with being the inventor of formal software inspections.
- This level of formality is normally found only in highly restrictive environments where code flaws may have a catastrophic impact.

Fagan Code Review Phases



Testing Methods

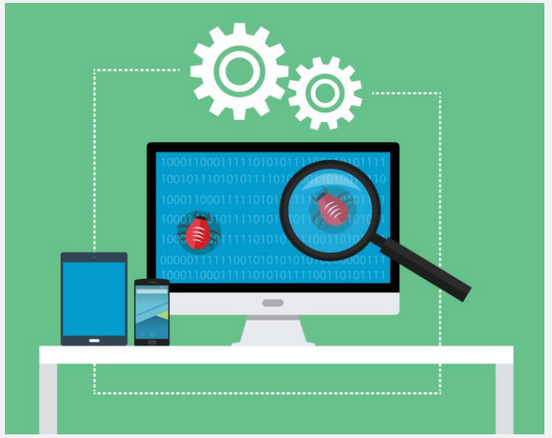
Static Testing

- It evaluates the security of a software without running it.
- It usually involves the use of automated tools designed to detect common software flaws such as buffer overflows.
- In mature development environments, developers are given access to static analysis tools to use them throughout the design, build, and test processes.
- It helps developers identify programming flaws and vulnerabilities.
- Static analysis can never reveal logical errors and design flaws.

Testing Methods

Dynamic Testing

- It evaluates security of software in a runtime environment and is often the only option for organizations deploying applications by someone else.
- Sometimes, testers do not have access to the source code.
- Dynamic testing can involve the use of synthetic testing.
- It is effective for compatibility tests, detect memory leakages, identify dependencies, and analyze software without having to access the software's actual source code.



Dynamic Testing

Dynamic Testing Methods

Fuzz testing is a specialized dynamic testing technique that provides different inputs to software to stress their limits and find previously unknown flaws.

Mutation (Dumb) Fuzzing

- Takes previous input values from actual operations of the software and manipulates them to create fuzzed input
- Might alter the characters of the content and append strings
- Example: ZZUF tool automates the process of mutation fuzzing

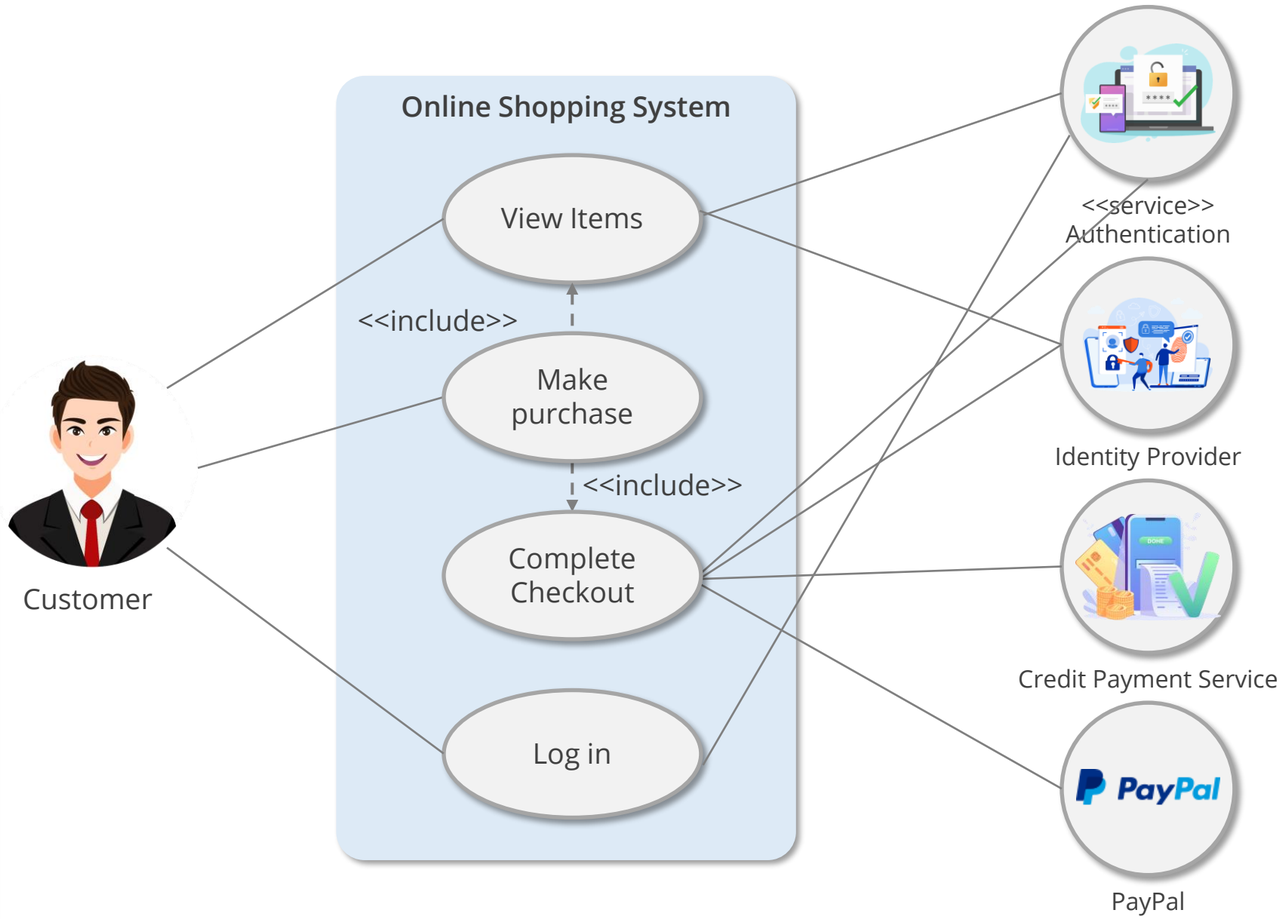
Generational (Intelligent) Fuzzing

- Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program
- Example: Peach Fuzzing Platform

Use Case Testing or Positive Testing

Use Case Testing or Positive Testing

- A use case describes the sequence of actions between the user and the system that result in an expected output.
- Use cases are textual but are graphically represented using the Unified Modeling Language (UML).
- Use cases are related to one another in a variety of ways called associations.
- Use cases are mainly helpful in determining the normal or expected behavior of a system rather than in assessing its security.



Misuse Case or Abuse Case Testing

- Misuse case is a use case that includes threat actors and the actions they want to perform on a system.
- Under UML, threat actors are represented as stick figures with shaded heads and their actions are depicted as shaded ovals.
- The misuse case is meant to threaten a specific portion or an illegitimate use case of the system.
- Misuse case testing helps to ensure one has effectively addressed each of the risks identified and has decided to mitigate them during the risk assessment phase.
- A misuse case doesn’t require including all the possible threats to the system, but it should include the ones which had to be addressed.
- Misuse cases are used by software developers to evaluate the vulnerability of their software to known risks.

Misuse Case or Abuse Case Testing

Misuse case testing scenarios

- Allowed data limits and bounds
- Populating the required fields
- Reasonable data
- Web session testing
- Allowed number of characters
- Correspondence between data and field types

Use Case vs. Misuse Case

Use Case

- System is verified using valid forms of input data
- Used to test whether the application works as expected
- Test fails if an error is encountered during testing

Misuse Case or Abuse Case

- System is verified against invalid input data
- Used to detect situations such as unexpected user behavior or invalid input and prevent applications from crashing
- Finds application's weak points and helps to improve its quality

Test Coverage Analysis

Test coverage involves a set of test cases written against the requirement specification.

- Test groups may refer to a percentage of the test cases that were run, passed, or failed.
- These are referred to as test coverage metrics.
- QA groups often use test coverage to implement test metrics according to the test plan.
- It is practically impossible to completely test a software.
- Testing professionals conduct test coverage analysis to estimate the degree of testing conducted against the new software.

It is computed using the formula:

Test coverage = the number of use cases tested or total number of use cases

This is a highly subjective calculation.

Code Coverage Analysis

Code coverage refers to how well the test set is covering the source code. That is, to what extent is the source code covered by the set of test cases.

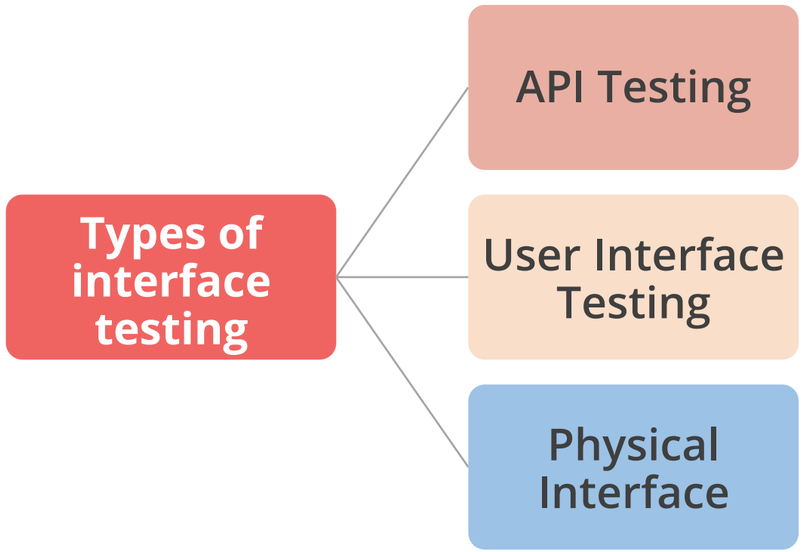
Different functionalities to be tested during code coverage:

- **Condition coverage**: All Boolean expressions to be evaluated for true and false
- **Decision coverage**: Not just Boolean expressions to be evaluated for true and false but to cover all subsequent if-else body
- **Loop coverage**: Every possible loop has been executed one time, more than once, and zero times
- **Entry and exit coverage**: Test for all possible calls and their return value
- **Parameter Value Coverage (PVC):** Check if all possible values for a parameter are tested
- **Inheritance coverage**: In case of an object-oriented source, when returning a derived object referred by base class, the coverage should be evaluated to check if the sibling object is returned

Interface Testing

An interface is an exchange point of data between the system and the user.

- It is performed to check if the different components of the application or system being developed are passing data and control correctly to one another.
- It helps to verify if all the interactions between components work correctly, check if errors are handled appropriately, and ensure high quality of software products.
- The testing should include known good and bad exchanges.
- It is a systematic evaluation of a given set of exchange points.
- Both testing and development teams perform this test.



Types of Interface Testing

Application Programming Interface (API)	• Offers a standard way for code modules to interact and be exposed to the outside world • Needs to be tested by developers to ensure they enforce all security requirements
User Interface (UIs)	• Graphical user interface and command-line interfaces that provide end-users with the ability to interact with the software • Test should include reviews of all user interfaces to verify that they function properly
Physical Interfaces	• Exist in some applications that manipulate machinery and logic controllers • Testers should pay careful attention to physical interfaces because of the potential consequences that might occur if they fail

Breach Attack Simulations

Gartner defines Breach and attack Simulation (BAS) as tools "*that allow enterprises to continually and consistently simulate the full attack cycle (including insider threats, lateral movement and data exfiltration) against enterprise infrastructure, using software agents, virtual machines, and other means*".

BAS testing mimics real-world attack scenarios to help organizations test and measure the effectiveness of their security controls and staff.

Key capabilities and functions of BAS:

- Can be deployed on-premise or on cloud
- Provides continuous, on-demand, or periodic testing
- Covers all phases of an attack, from pre-exploitation to post-exploitation, persistence, and maintaining access
- Includes testing for both perimeter and internal security controls
- Comprehensive reports include recommendations for mitigation

Compliance Checks

Compliance checking is the process of review and analysis of the implemented controls to check whether the implemented controls follow regulations, laws, and policies.

Regulatory compliances include PCI-DSS, FISMA, GLBA, SOX, ISO 27001, and HIPAA.

Collect Security Process Data

Account Management

Account management involves provisioning, deprovisioning, and periodic reviews of user accounts, access rights, and privileges of employees and vendors.

This data collection also includes verification of the account provisioning process along with the verification of the accounts' privileges.

Accounts should be processed through a comprehensive verification mechanism, which includes an authorized sign-off from the management and other assurance techniques.

Account Management

Deprovisioning of accounts should also pass through an appropriate process based on the organization's requirements.

Deprovisioning should include access removal in the case of an employee leaving the company, account adjustments in the case of change in designations, and a review of the accesses given to individuals.

Management Review and Approval

"Top management shall review the organization's information security management system (ISMS) at planned intervals to ensure its continuing suitability, adequacy, and effectiveness."

~ ISO 27001:2013 Management review

Key Performance Indicators (KPIs)

It is a process by which the performance of security controls and processes is measured.

ISO 27004 deals with KPI metrics.

KPIs should be understandable to both business and technical audiences and should be aligned with one or more organizational goals.

Key Terms Associated with KPI

These are some of the important terms associated with KPI:

Factor

- An attribute of the ISMS that can be described as a value that can change over time
- Example: Several AV alerts or a few investigations conducted

Measurement

- The value of a factor at a particular point in time
- This is the raw data
- Example: 20 AV alerts per day or 15 investigations per month

Baseline

- An arbitrary value for a factor that provides a point of reference or denotes that some condition is met by achieving some threshold value
- Example: The number of AV alerts per month will not be more than 25 or the number of investigations open for more than 48 hours should not be more than 10

Key Terms Associated with KPI

Metric

- A desired value that is generated by comparing various results with each other or with the baseline
- Example: The ratio of false-positive AV alerts to valid alerts per month

Indicator

- An interpretation of one or more metrics that describes the effectiveness of an element of the ISMS
- Indicators are meaningful to management

KPI Process

A KPI process includes:

- Choosing the factors that can show the state of security
- Defining baselines for some or all factors under consideration
- Developing a plan for periodically capturing the values of these factors
- Analyzing and interpreting the data
- Communicating the indicators to all stakeholders

Key Risk Indicator (KRI)

- KRIs indicate where an organization is in relation to its risk appetite.
- They measure how risky an activity is so that leadership can make informed decisions about the activity.
- KRIs are selected for their impact on the decisions of the senior leaders in an organization.
- It is useful to relate them to SLE equations.
- KRI's alert the organization when an unfavorable situation might arise, which allows the organization to plan for these situations.

Key Performance and Risk Indicators

Key performance indicator

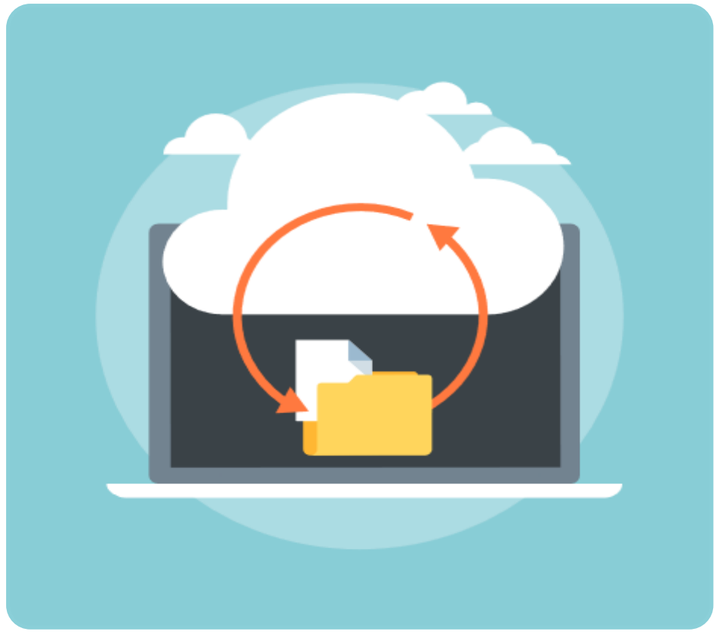
- A key performance indicator (KPI) measures how well something is being done.
- Some parameters used as KPIs are cost adherence, schedule adherence, and project effort adherence.

Key risk indicator

- Key risk indicator (KRI) is a measure used in management to indicate how risky an activity is or the possibility of an adverse impact in the future.
- KRIs use mathematical formulas or models to give an early warning of a potential event that may harm the continuity of the activity or project.

Backup Verification Data

- IT contingency plans should include a method for conducting data backups frequently.
- Periodic backups can be scheduled via an automated backup management system or an automated job scheduling software.
- The stored data should be routinely tested to validate the backed-up data's integrity.



Security Education Training and Awareness

- SETA is the process of informing employees about security best practices.
- The goals of security awareness programs are to reduce risks by addressing the behavioral element of security through education and consistent application of awareness techniques.
- Security awareness programs should focus on common user security concerns such as password selection, appropriate use of computing resources, and social engineering attacks.
- Security programs should be tailored to the target audience.

Analyze Test Output and Generate Report

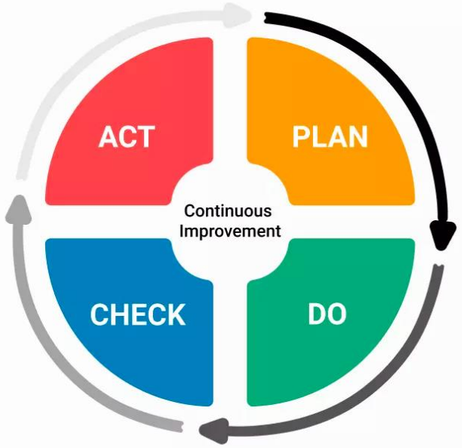
Remediation

Continuously monitoring an organization's security posture is a good start in building a mature security program.

Organizations should try to adopt a *continuous process improvement* model, such as the **Deming (PDCA) cycle,** to improve their security posture.

The principles for continuous improvement of cybersecurity are:

- Make small changes to yield significant improvements
- Seek employees' feedback to identify opportunities for improvements
- Empower employees to take ownership for improvements
- Identify key metrics to measure improvements



Exception Handling

Exceptions to any information security policies or procedures should be documented, authorized, and reviewed.

The exception should be approved or denied after carefully reviewing the request.

An exception request should be made by the related individual to the security management with proper justification.

Ethical Disclosure

Nondisclosure is the practice of containing the vulnerability and its existence from the general public due to nondisclosure or other contractual agreements.

Ethical Disclosure

- **Full disclosure** is the practice of publishing analyses of software vulnerabilities as soon as possible to all potentially affected organizations.
- The primary purpose of disclosing information about vulnerabilities is so that organizations at risk can take appropriate actions to protect themselves.

Ethical Disclosure

Responsible disclosure is the practice of reporting a vulnerability to the vendor and allowing them some time to fix the vulnerability before informing the public.

Ethical Disclosure

Mandatory reporting is when the law requires one to report known or suspected cases of fraud, data breaches, and computer crimes to the relevant authorities.

Ethical Disclosure

Whistleblowing is the act of notifying senior management, industry regulators, government authorities, or the general public regarding any breaches, unethical actions, and illegal behaviors of their employer.

Real World Scenario

Google’s Project Zero is a team of dedicated security analysts tasked with finding zero-day vulnerabilities. Project Zero was announced on July 15, 2014, on Google's security blog.

Project Zero has been responsible for identifying serious security flaws such as Meltdown and Spectre.

Bugs found by the Project Zero team are reported to the vendor and made publicly available only after 90 days from the day the bug is discovered.

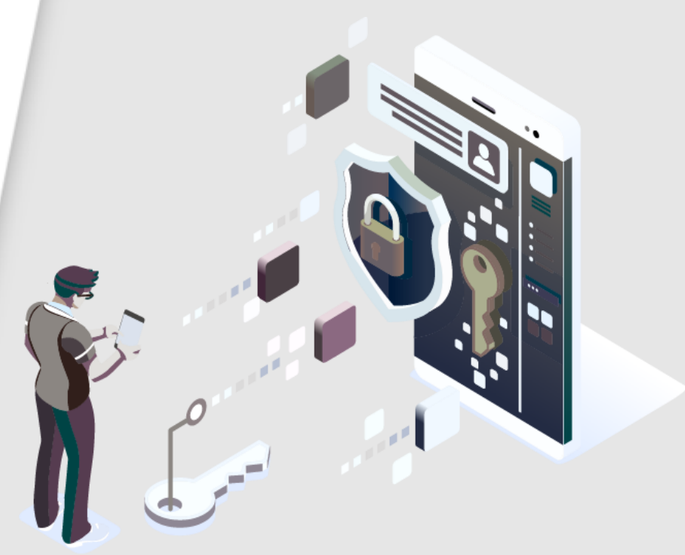
If the vulnerabilities are patched within 90 days, technical details are disclosed 30 days after the release of a fix to give users time to install the patch.

The 90-day deadline is Google's way of implementing responsible disclosure, giving vendors 90 days to fix a problem before informing the public so that users themselves can take the necessary steps to avoid attacks.

Information source: https://googleprojectzero.blogspot.com/2021/04/policy-and-disclosure-2021-edition.html
And
https://github.com/googleprojectzero

Key Takeaways

- Security assessment and testing maintain a system's ability to deliver its intended functionality securely by evaluating the information assets and associated infrastructure.
- Various tools and techniques are used to identify and mitigate risks due to design flaws, architectural issues, hardware and software vulnerabilities, coding errors, and other weaknesses.
- Security policies and procedures are uniformly and continuously applied.
- The security professional should be capable of validating assessment, testing strategies, and carrying out those strategies using various techniques.
- In the absence of careful analysis and reporting of assessment results, security assessments and testing have little value.



This concludes **Security Assessment and Testing.**

The next domain is **Security Operations.**