Certified Information Systems Security Professional (CISSP) Certification Training Course

CISSP® is a registered trademark of (ISC)² ®

Domain 06: Security Assessment and Testing

Learning Objectives

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

- Apply assessment, testing, and audit strategies to evaluate organizational effectiveness
- Interpret penetration testing and log management phases to identify vulnerabilities
- Differentiate testing techniques and methods to determine their suitability
- Establish KPIs and evaluate their impact on performance
- Compare approaches to ethical disclosures to ensure compliance

Introduction to Security Assessment and Testing

Security Assessment and Testing

It is performed to identify the current security status of an information system or an organization.

It identifies the technical, operational, and system deficiencies early.

It provides recommendations for improvement allowing the organization to achieve security goals that mitigate risk.

It ensures that appropriate and timely corrective actions are applied before deploying the system in the production environment.

Security Assessment and Testing

The different types of security assessments include:

Vulnerability assessment

Penetration testing

Security audits

Design and Validate Audit, Assessment, and Test Strategies

Risk Audit

It provides reasonable assurance that adequate risk controls exist and are operationally effective.

It is a systematic, repeatable process where a competent, independent professional:

- Evaluates one or more controls
- Interviews personnel
- Obtains and analyzes evidence
- Develops a written opinion on the effectiveness of the control(s)

Types of Audit

Internal audit

- It is performed by an organization’s internal staff.
- The reports are intended for an internal audience.
- Auditors may have a hidden agenda and can lead to a conflict of interest.
- It is not expensive.

External audit

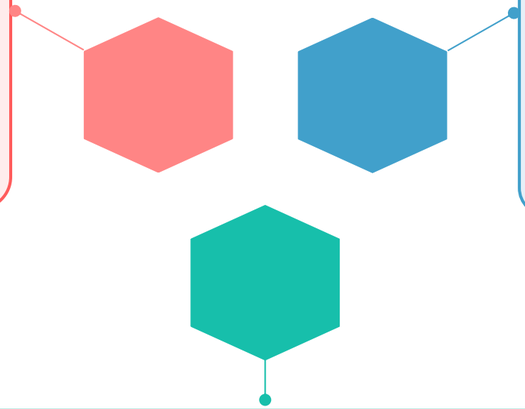
- It is performed by third-party auditors.
- The reports are intended for third-party stakeholders.
- Auditors are unaware of the internal dynamic and politics.
- It is more expensive to conduct an external audit.
- An NDA must be signed for an external audit.

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 to improve the effectiveness of its 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 lifecycle.

Factors driving the audit

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

Audit Process

The audit process occurs as described below:

01

Determine the goal of the audit

02

Bring in stakeholders at the earliest stage possible and identify and address the business needs

03

Define the scope of the assessment

04

Choose the right audit team based on the goals, scope, budget, and available expertise

Audit Process

05

Ensure all goals are met on time and within the budget

06

Stick to the plan and document deviations

07

Document the results from the beginning of the planning process to the results

08

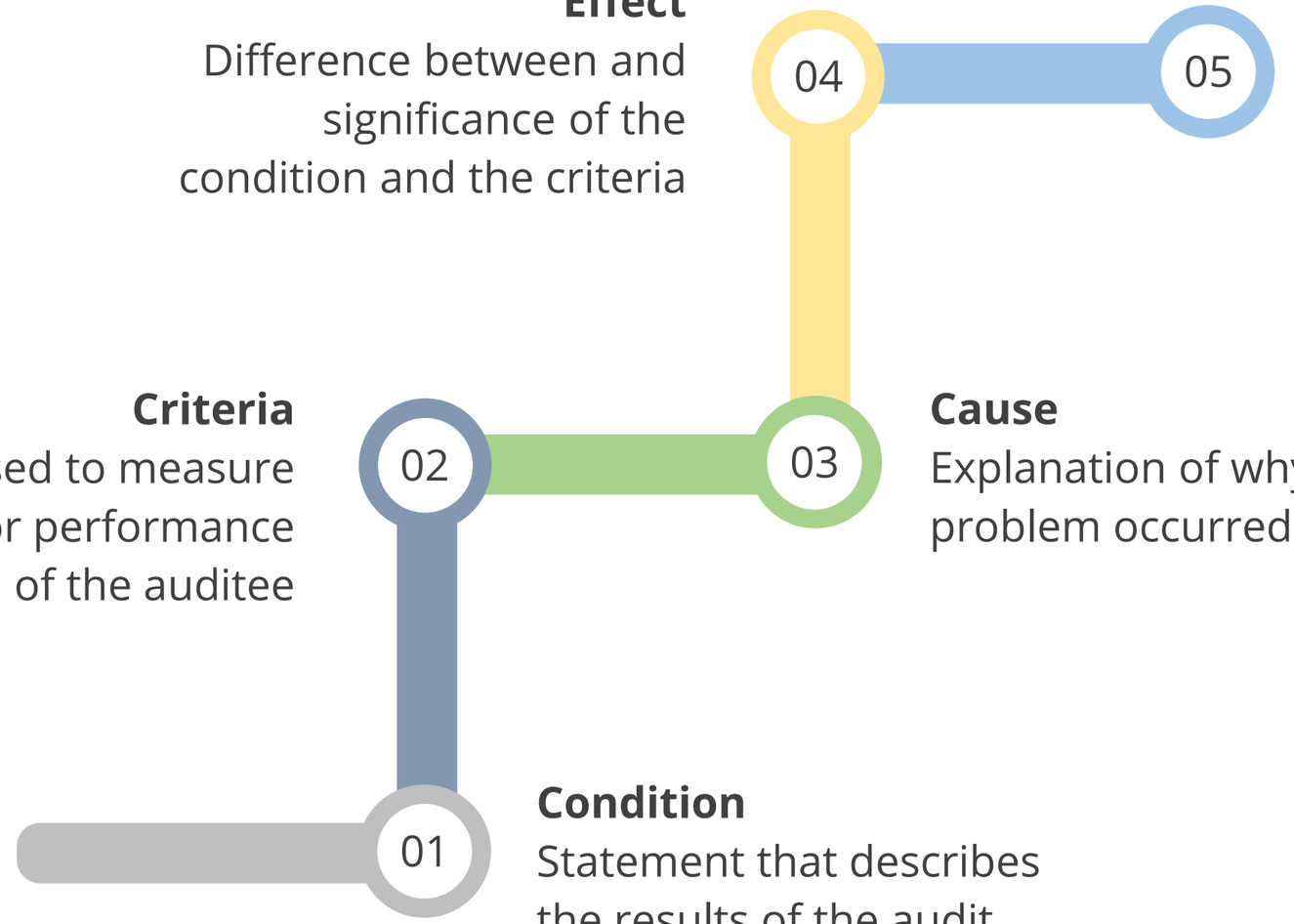
Communicate to the right leaders to achieve and sustain a strong security posture

Elements of an Audit Finding

The results of the audit have the following five elements:

Effect
Difference between and significance of the condition and the criteria

Recommendation
Action that must be taken to correct the cause



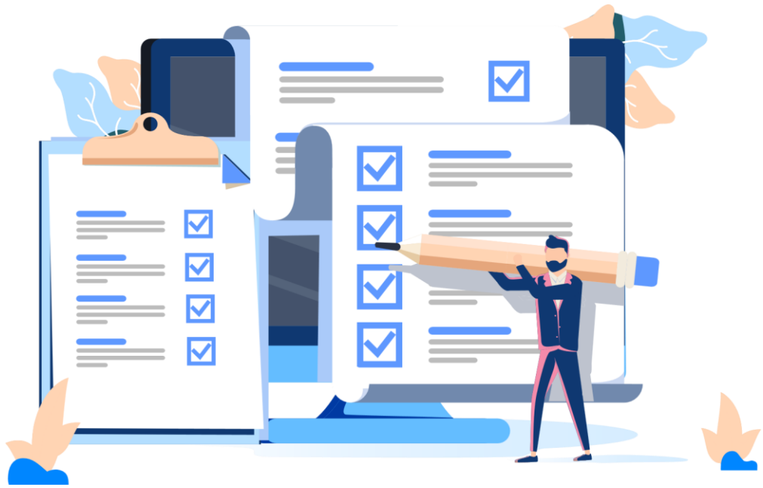
Criteria
Standards used to measure the activity or performance of the auditee

Cause
Explanation of why a problem occurred

Condition
Statement that describes the results of the audit

Assessment

It 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).

Informal assessments are performed by internal assessors and rely on documented and established organizational processes to improve the controls' effectiveness and efficiency.

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

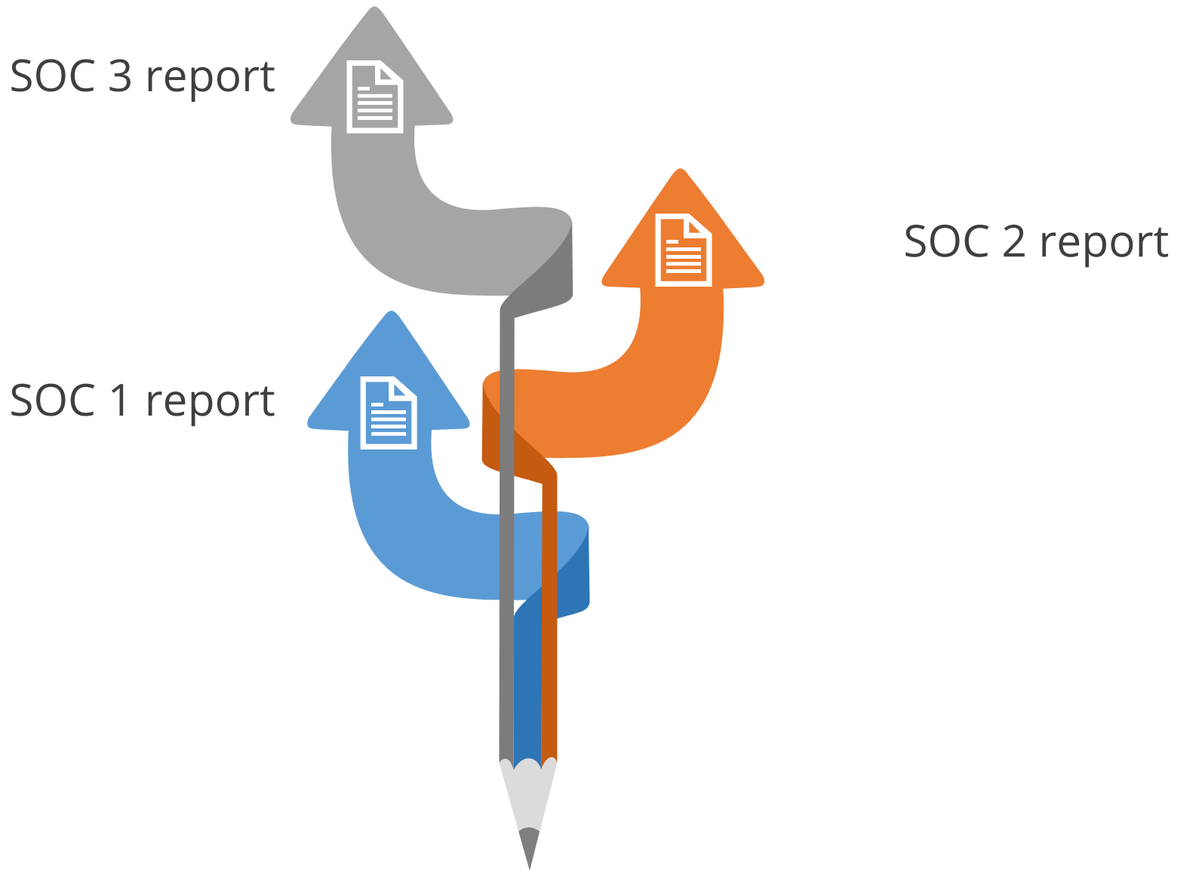
SOC (Service Organization Control) Reports and Security Assessments

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

- They are designed to help service organizations and organizations that provide information systems services to other entities.
- They help build customer trust and confidence in their service delivery processes and controls.
- They are created by an independent certified public accountant (CPA).

SOC Reports and Security Assessments

The following types of SOC reports help service organizations meet specific user needs:



SOC 1 Report

It is a report relevant to user entities' internal control over financial reporting and is prepared under SSAE 18, enhancing the previous SAS 70 standard.

There are two types of SOC 1 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 specific period, such as 6 months.

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

SOC 2 Report

It covers security, availability, processing integrity, confidentiality, or privacy of a service organization’s controls.

There are two types of SOC 2 reports based on the Trust Services Principles and illustrations criteria:

Type 1: Based on a service organization’s system and the suitability of the design of controls

Type 2: Based on 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 Report

It is based on trust criteria modeled around four broad areas:

Policies

Communications

Procedures

Monitoring

The principles and criteria are jointly set by the AICPA and Canadian CPAs.

SOC 2 Report

The trust services criteria are:

Security	Protects the system against unauthorized access, use, or modification, both physical and logical
Availability	Ensures the system is available for operation and use as committed to or agreed upon
Integrity	Verifies that system processing is complete, valid, accurate, timely, and authorized
Confidentiality	Protects information designated as confidential as committed to or agreed upon, particularly sensitive business information
Privacy	Confirms that the system’s collection, use, retention, disclosure, and disposal of personal information meet commitments in privacy notices

SOC 3 Report

It is a type of attestation report that provides a general-use opinion on a service organization's controls relevant to security, availability, processing integrity, confidentiality, or privacy.

It is designed for users who need assurance about the controls but do not require the detailed information provided in a SOC 2 report.

SOC 1, SOC 2, and SOC 3 Comparison

	Purpose	Intended users	Focus	Report type	Evaluation
SOC 1	Financial statements	Financial statements auditors, customers, and related third parties	Internal controls relevant to financial reporting	Type I and Type II	Design of internal control, operating effectiveness of internal control during review period
SOC 2	GRC programs, oversight, and due diligence	Management, regulators, and related third parties	Operational controls regarding security, availability, processing integrity, confidentiality, or privacy	Type I and Type II	Design of internal control, operating effectiveness of internal control during the review period
SOC 3	Marketing or general purpose	Anyone with a need for confidence in service organizations controls	Report on controls that are easy to read	General	Design of controls related to SOC2 objectives

Source: https://accedere.io/soc-reporting-services.html

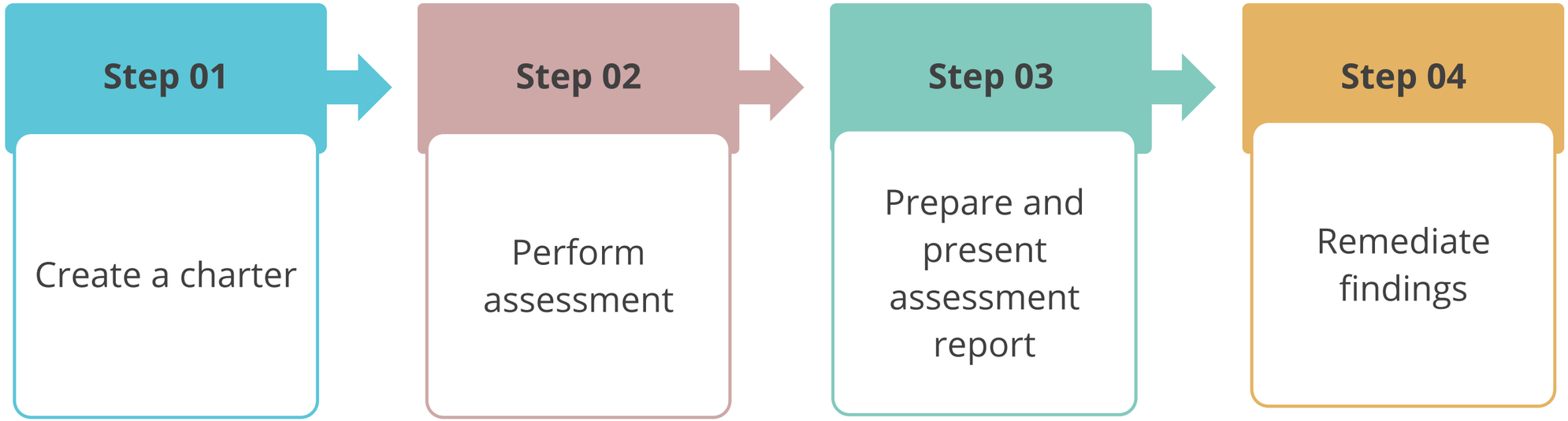
Internal Assessment

It is used to determine if the security controls meet the organization’s risk expectations.

It 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

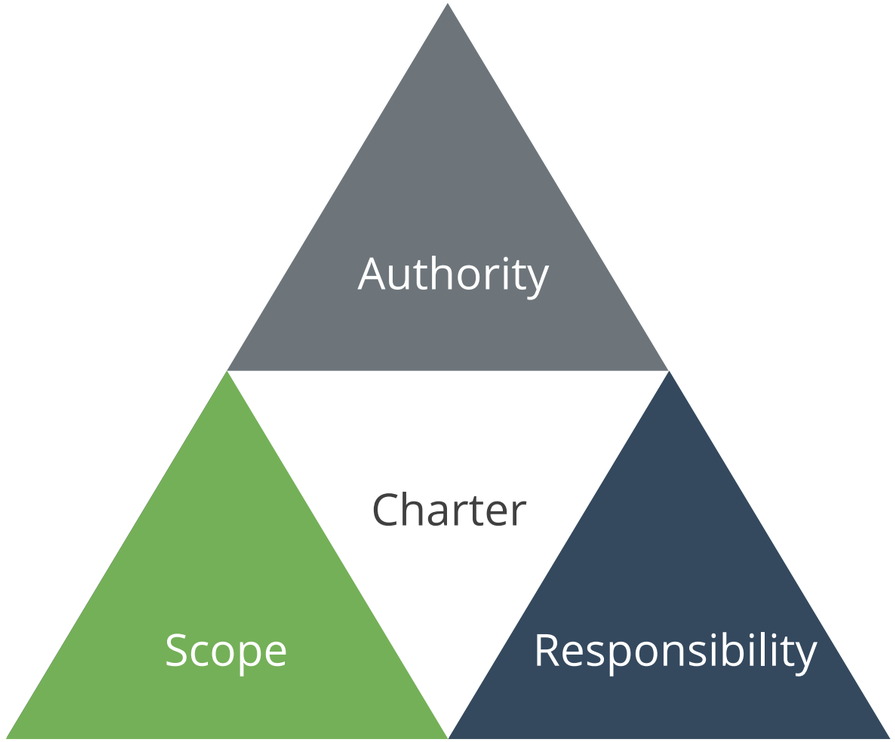
Steps to Conduct Internal Assessment



Charter

It 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.
- The management must define the scope of assessment.



Scope of Assessment

It includes the **people**, **processes,** and **technologies** used to support a business and address the following controls:

- Physical
- Technical
- Administrative

Scope of Assessment

There are two kinds of assessments based on the scope:

Vulnerability assessment

- It identifies the vulnerabilities in IT and evaluates the risks with these vulnerabilities.

Penetration test

- It evaluates the system security in a realistic simulation of an attacker who intends to break into a target system.
- It not only identifies likely weaknesses but also tries to exploit the potential weakness.

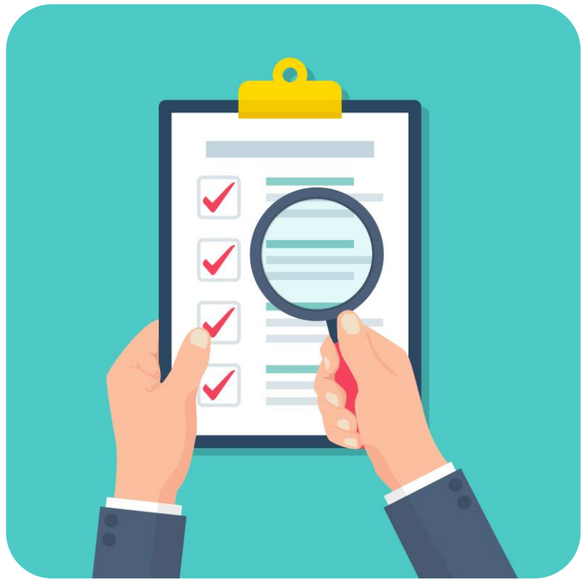
Assessment Report

- It documents the process followed, observations, evidence, findings, conclusions, and recommendations in the assessment report.
- It is presented to relevant levels of senior management.
- Its exact format varies depending on the organization.
- It adjusts the levels of detail presented based on audiences.
- It contains 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.



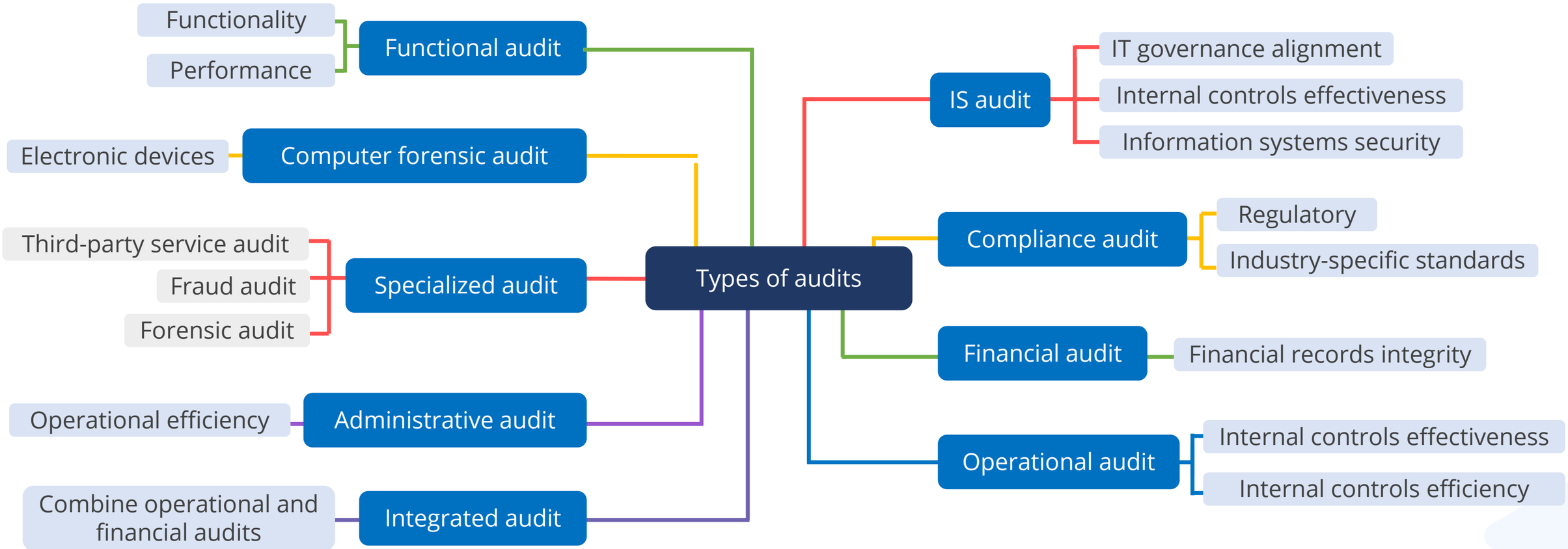
Based on the findings:

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

Plan of Action and Milestones (POAM) is a document that identifies tasks for remediation, resources required, key milestones, and scheduled completion dates for the milestones.

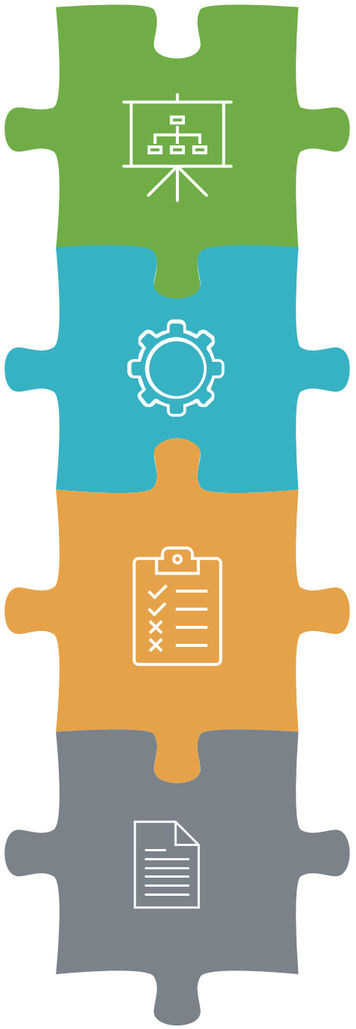
Types of Audits

The following diagram illustrates different types of audits and what they assess:



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

Steps to Conduct an External Audit



Create an audit charter

Plan audit

Perform audit

Prepare and present audit report

Audit Planning

It is an important activity for both internal and external audits.

An audit plan is a project plan that helps 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 and coordinate audit activities with the client

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

Third-Party Audit and Assessment

It 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 are:

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

Principles of Supply Chain Security

Four principles of supply chain security are:

I. Understand the risks

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

II. Establish controls

- Communicate the security needs to the suppliers
- Set and communicate minimum security requirements for the suppliers
- Build security considerations into the contracting processes and mandate suppliers do this too
- Meet the security responsibilities as a supplier and consumer
- Raise awareness of security within the supply chain
- Provide support for security incidents

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

Principles of Supply Chain Security

III. Check the arrangements

- Build assurance activities into the supply chain management approach

IV. Improve continuously

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

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

Testing

It is important to test the security controls for their effectiveness.

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

Substantive testing (test of details): 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.

Quick Check

You are an auditor preparing to conduct a comprehensive audit of your organization. Before initiating the process, which of the following will ensure that you have the necessary authority to carry out the audit effectively?

A. An approved audit plan

B. An approved audit charter

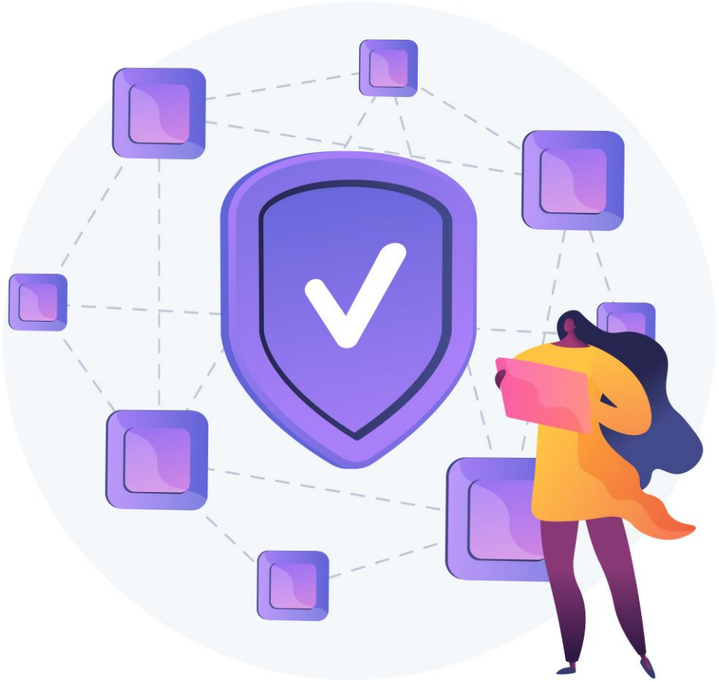
C. An approved audit schedule

D. An approved audit program

Vulnerability Assessment and Penetration Testing

Vulnerability Assessment

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



Its objective is to detect and remediate vulnerabilities in a timely fashion.

Vulnerability Assessment

The steps in this process are:

1. Identify the assets or resources
2. Assign a quantifiable level of importance to the identified resources
3. Discover vulnerabilities or potential threats to each resource
4. Develop a strategy to mitigate or eliminate the most serious vulnerabilities in the most valuable resources
5. Define and implement ways to minimize the consequences if an attack occurs

Types of Vulnerability Assessments

Personnel testing

- Identify vulnerabilities in standard employee practices and demonstrate social engineering attacks

Physical testing

- Review facility and perimeter protection mechanisms
- Perform physical security vulnerability assessments

System and network testing

- Assess the system using the following methods:
  - Network discovery scan
  - Network vulnerability assessment
  - Web application vulnerability scan

Network Discovery Scan

It is a foundational step in the vulnerability assessment process, providing critical visibility into the network landscape.

- It searches for systems with open ports.
- It does not probe systems for vulnerabilities.

Commonly used tools

- NMAP
- Angry IP Scanner

Network Discovery Scan

There are four network discovery scanning techniques:

TCP SYN scanning

- It sends a single packet to each scanned port with the SYN packet set.
- A response with SYN and ACK flags indicates the port is open at the sender's end.
- It is also called half-open scanning.

TCP connect scanning

- It opens a full connection to a remote system on the specified port.
- It is used when the user running the scan does not have the necessary permissions to run a half-open scan.

TCP ACK scanning

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

Xmas scanning

- It sends a packet with the FIN, PSH, and URG flags set.

Network Vulnerability Scan

It is a vital component of a comprehensive cybersecurity strategy, helping organizations identify, assess, and remediate vulnerabilities to protect their networks and data from potential threats.

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**: Identifying a vulnerability and failing to report it as a part of the results, leading to a dangerous situation

Tools used

- Tenable Nessus
- OpenVAS
- Microsoft baseline security analyzer (MBSA)
- Retina network scanner community edition

Network Vulnerability Scan

Types of scans

Unauthenticated or non-credentialed scan:

- Identifies a network or a networked system for vulnerabilities that are accessible without logging in as an authorized user
- Inspects the security of a target system from an outsider’s perspective

Authenticated or credentialed scan:

- Tests vulnerability as a logged-in or authenticated user
- Helps in reducing the false-positive and false-negative results
- Scans servers with read-only access

Benefits of Network Vulnerability Scan

Identify weak points: Provides a comprehensive view of potential vulnerabilities within the systems

Prioritize remediation: Categorizes vulnerabilities based on severity (using CVSS) and helps organizations prioritize the issues

Monitor continuously: Issues an ongoing assessment of the security posture, addressing emerging threats and vulnerabilities proactively in real time

Vulnerability Scanners

They continuously identify, analyze, and report on potential security weaknesses in an IT infrastructure.

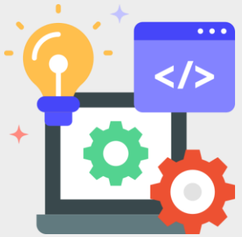
They work by comparing information about the software running on a system (such as version numbers and configurations) against databases of known vulnerabilities.

Vulnerability Scan Process

Vulnerability scanner

1 Sends probe

2 Analyzes response



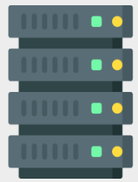
Target system

3 Records response

4

- Open SSL 3.0
- Nginx 1.19.2
- Open SSH 8.3

5 Correlates to known security vulnerabilities



Vulnerabilities database

Vulnerability Analysis

It is a central component in cybersecurity that balances data collection and actionable decision-making.

Analysis transforms raw data about vulnerabilities and threats into comprehensive insights.

Confirmation of Vulnerabilities

It involves a rigorous process to validate suspected vulnerabilities.

False positive

Can act as a smokescreen, hiding a real issue by overwhelming a security team with false alarms

False negative

Can be even more damaging, serving as a ticking time bomb for unauthorized access to critical systems

Analysts confront false positives and false negatives, reflecting the accuracy of prior vulnerability assessments.

Vulnerability Classification

It is the organized categorization of identified vulnerabilities within a system or application.

Classification is usually done based on:

- Nature of a vulnerability
- Level of risk it poses
- Component affected
- Potential impact

Vulnerability Classification Factors

- Exposure factor
- Environmental variable
- Industry impact
- Risk tolerance

Prioritization

It is the process of categorizing vulnerabilities based on their potential impact and the severity of the risk they pose.

It is a complex juggling act that requires a deep understanding of cybersecurity principles and the organization’s operational intricacies.

Common Vulnerability Scoring System (CVSS)

It assesses the severity of vulnerabilities, according to factors such as the impact, exploitability, and ease of remediation.

It provides a robust mechanism for assessing vulnerabilities in a standardized way.

It quantifies the nature and severity of software vulnerabilities.

It helps security professionals and organizations in making informed decisions about risk mitigation.

Score	Rating
9.0-10.0	Critical
7.0-8.9	High
4.0-6.9	Medium
0.1-3.9	Low

CVSS Scoring

Assessment of vulnerabilities is done based on the following factors:

Temporal metric: It examines the attributes of a vulnerability that may change over time, including exploit code maturity, remediation level, and report confidence.

Base metric: It is the inherent quality of a vulnerability and is independent of any specific system or environment.

Environmental group: It allows an organization to tailor CVSS scores based on specific environmental characteristics, providing a customized risk assessment.

Common Vulnerabilities and Exposures (CVE)

It identifies and catalogs publicly disclosed cybersecurity vulnerabilities, aiming to standardize their identification and improve communication and collaboration among:

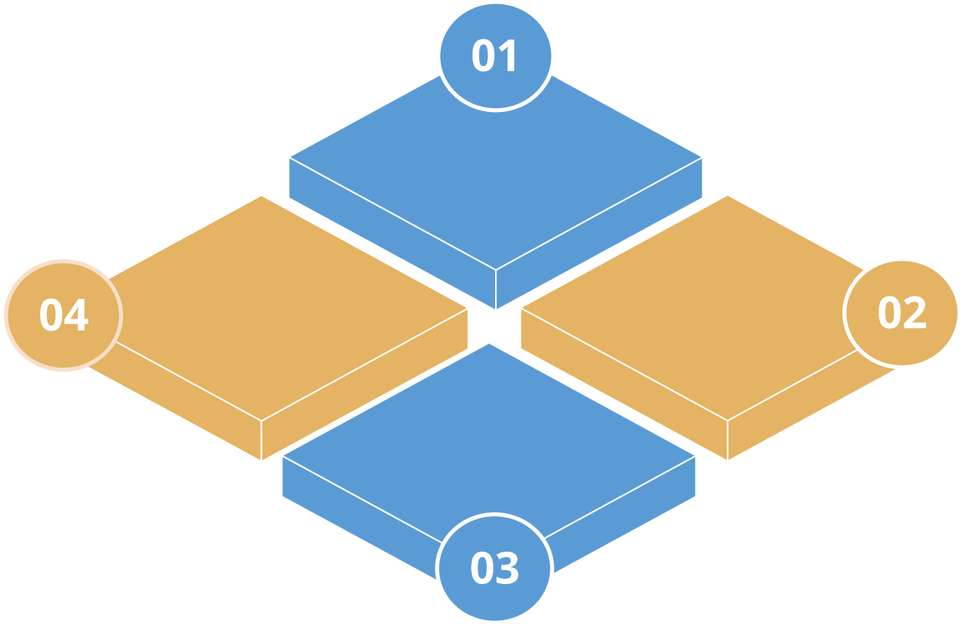
Software vendors

Cybersecurity professionals

Other stakeholders

CVE Details

Severity score:
An indication of the vulnerability's severity using a scoring system like CVSS



Public references:
An additional link to resources like exploit code, vendor advisories, or mitigation strategies

Description:
A detailed explanation of the vulnerability, its potential impact, and affected systems

CVE ID:
A unique identifier in the format cve-yyyy-nnnn
(Example: Cve-2023-4567)

Vulnerabilities Response and Remediation

Patching	• It updates software, applications, and systems to address known vulnerabilities. • It bolsters an organization’s defense by closing security gaps that malicious actors may exploit.
Insurance	• It serves as a financial safety net, providing coverage for potential losses resulting from cyber incidents.
Segmentation	• It divides a network into isolated segments, limiting lateral movement for attackers, and containing potential breaches. • It minimizes the impact of a cyber breach.

Validation of Remediation

Rescan

Reruns vulnerability scans after applying patches or making other changes

Verification

Involves ongoing monitoring and assurance that vulnerabilities remain mitigated over time

Audit

Offers a thorough manual review by an independent third party or internal team, unlike automated rescans

Reporting

It is a formal document that details security weaknesses in software applications, systems, or components.

These reports are generated by vulnerability scanning systems and serve as actionable insights and organizational memory for cybersecurity efforts.

Components of Reporting

Vulnerability overview

Summarizes current vulnerability landscape, including the total number of vulnerabilities, their severity distribution, and trends over time

CVSS score

Relates detailed information on the varying levels of severity for identified vulnerabilities, and highlights the ones that require immediate attention

Remediation progress

Updates the status of remediation efforts, including the number of vulnerabilities addressed and those still pending

Risk metric

Includes metrics to measure vulnerability management activities that have contributed to reducing the organization’s overall cybersecurity risk

Recommendation

Provides clear recommendations on the prioritization and allocation of resources for vulnerability remediation efforts

Security Content Automation Protocol (SCAP)

It is a framework that enables compatible vulnerability scanners to see whether a computer adheres to a predefined configuration baseline.

It is a set of specifications and tools that standardize how information about software flaws, security configurations, and vulnerabilities is communicated and exchanged.

SCAP Attributes

01

Standardized formats: It defines formats for vulnerabilities, security configurations, and patching information to ensure compatibility across security tools.

02

Automation: It facilitates automation of vulnerability management tasks, including scanning, configuration assessment, and patch deployment.

03

Open source and vendor-neutral: It is an open-source and vendor-neutral approach that enables interoperability between security tools from various vendors.

Components of SCAP

Open vulnerability and assessment language (OVAL)

It structures vulnerabilities and configurations in a machine-readable format, facilitating interoperability between security tools.

Extensible configuration checklist description format (XCCDF)

It provides a standard format for security checklists, enabling different tools to understand them.

Common vulnerability scoring system (CVSS)

It assesses vulnerability severity and helps prioritize based on its potential impact.

SCAP Benefits

Improved efficiency
Automates vulnerability management tasks, saving time and resources

Simplified compliance
Helps organizations comply with security regulations and standards that require vulnerability management practices

Enhanced security
Ensures consistent and accurate communication of security information, leading to better decision-making

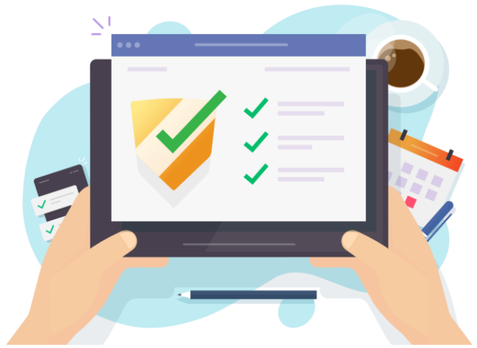
Vendor agnosticism
Allows use of various security tools from different vendors without compatibility issues

Web Application Vulnerability Scan

It is an automated security tool specifically designed to identify security vulnerabilities in web applications.

It uses special-purpose scanners that analyze web applications for known vulnerabilities.

Web Application Vulnerability Scan



In an ideal scenario, the scanner must:

- Conduct an initial scan of all applications
- Examine any new application before moving to production
- Inspect any modified application before it moves to production
- Perform regular and scheduled reviews of all applications

Web Application Vulnerability Scanning Process

Crawl and discover

Examine a website thoroughly, mimicking user or search engine bot interactions

Test for vulnerabilities

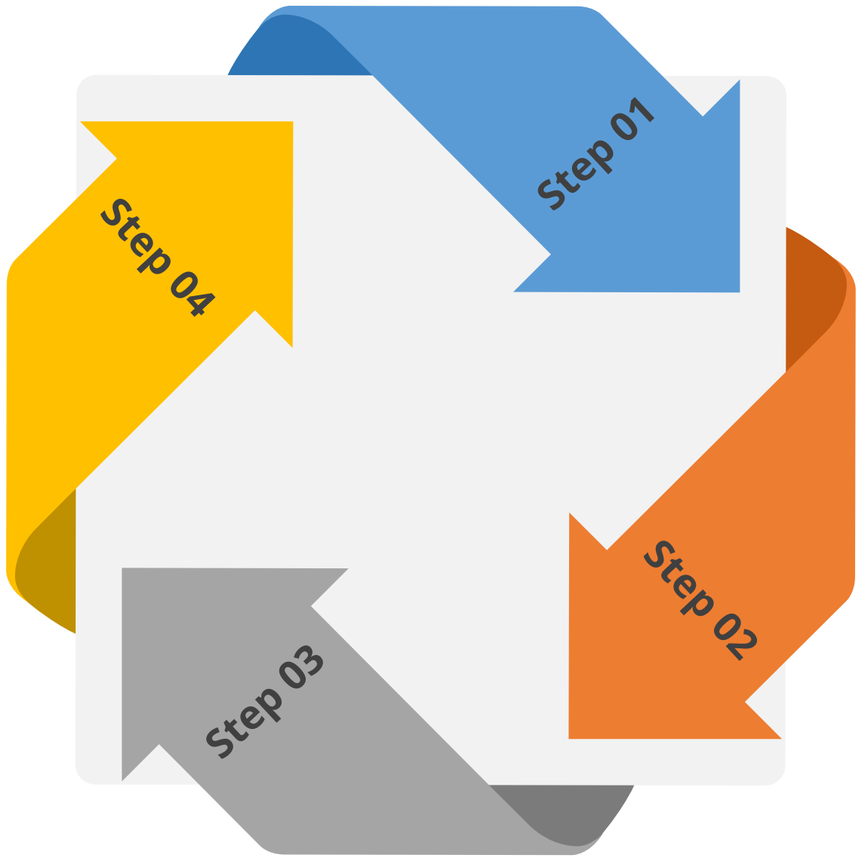
Assess potential weaknesses in the network, applications, and systems

Identify security misconfigurations

Identify insecure configurations, including outdated software and weak encryption settings

Generate reports

Generate a report detailing the identified vulnerabilities



Benefits of Web Application Scanners

Proactive security

Identifies vulnerabilities before exploitation to protect websites and user data

Improved security posture

Addresses vulnerabilities to strengthen web application security

Compliance with regulations

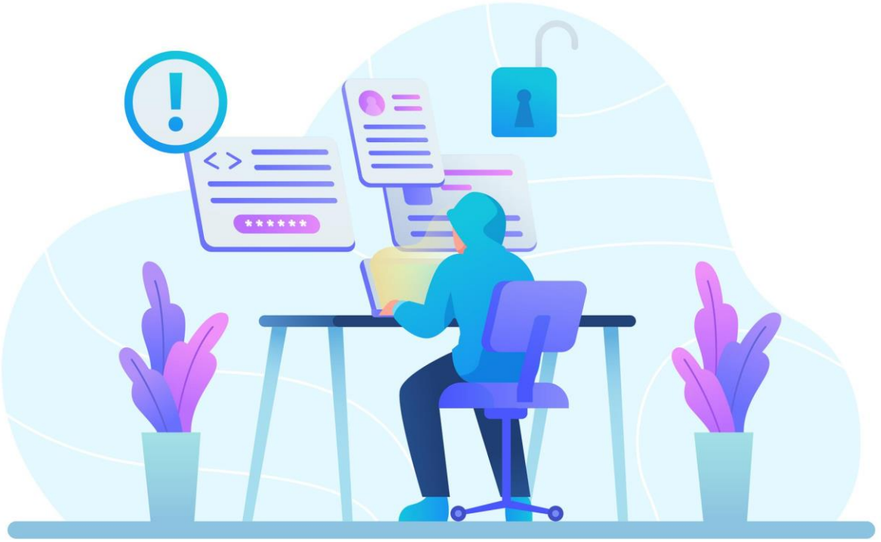
Adheres to regulations and standards by regularly scanning web applications for vulnerabilities

Reduced development costs

Detects vulnerabilities early in development to fix them more easily and cost-effectively than after a breach

Penetration Testing (Pen Testing or Ethical Hacking)

It is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit.



It determines the true nature and impact of a given vulnerability by exploiting existing vulnerabilities.

Tools required: Metasploit, Kali Linux, and Aircrack-ng

Penetration Testing Process

The phases of penetration testing are:

Discovery

Gathers information about the target

Enumeration

Performs port scans and resource identification

Vulnerability mapping

Identifies vulnerabilities in the systems and resources

Exploitation

Attempts to gain unauthorized access by exploiting vulnerabilities

Reporting

Communicates the findings to the management

Penetration 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 may not detect all vulnerabilities.
- It may inadvertently impact another system.

Penetration 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 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 is provided with information about how the internal system works.
- It helps guide their tactics toward areas that need to be thoroughly tested.
- It mitigates the risks of the other two models.

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

Penetration 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 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.

Quick Check

You have been asked to perform a penetration test for a bank. To make the test as realistic as possible, you have not been provided with any information about the bank other than the name and address. What type of penetration test will you perform?

A. A black-box penetration test

B. A dark-box penetration test

C. A white-box penetration test

D. A grey-box penetration test

Log Management

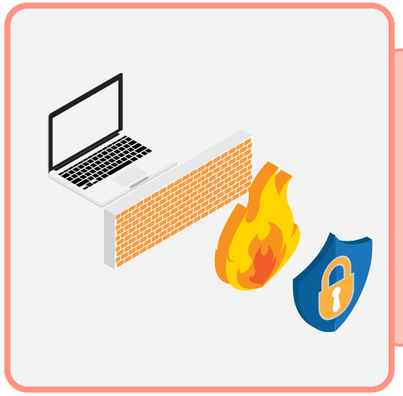
Log Management

It is the process of collecting, storing, and analyzing log data from various systems, applications, and devices within an organization.

Event Logs

In IT, they provide information about network and system traffic, and other conditions.

They store data for retrieval, aiding IT administrators in managing security, performance, and transparency.



Logs are also generated from antivirus software, firewalls, and intrusion detection and prevention systems.

Log Management and Review

They are the processes and policies used for 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 the 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 generation

Logs are generated from different devices and systems.

Log transmission

Logs are transmitted to some separate storage or log server.

Log storage

Logs are stored securely in some centralized log server.

Log analysis

Logs are analyzed to detect incidents or for forensic purposes.

Log disposal

Logs are disposed of securely once they have lived their life cycles.

Log Tampering Prevention

It is vital to maintain the integrity of log data, and the following methods prevent log tampering:

Remote logging	Places a log file on another device to protect it from tampering in a compromised system
Simplex communication	Uses a one-way communication between reporting devices and the central log repository, severing the **receive** pairs on an ethernet cable
Replication	Makes multiple copies and keeps them in different locations
Write-once media	Uses write-once media to prevent unauthorized modifications to log files
Cryptographic hash	Detects unauthorized modifications easily with this powerful technique

Log Management: Benefits and Challenges

Benefits

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

Challenges

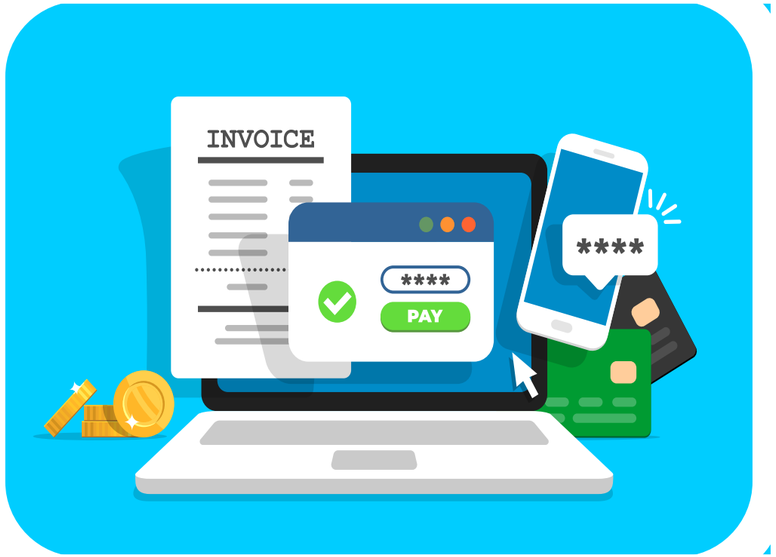
- Managing large quantities of logs from various sources
- Discrepancies in log content, timestamps, and formats

Log Management: Best Practices

- Establish log management policies and procedures
- Prioritize requirements for the 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

They enable organizations to identify and mitigate vulnerabilities more effectively.



Real transaction

- It is initiated by an end-user.

Synthetic transaction

- It is an automatic script-based transactions with an expected output.
- 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.
- It is an effective way of testing the software from outside.

Real User Monitoring and Synthetic Transaction

Real user monitoring (RUM)

- It is a passive monitoring technology that checks if users are served correctly and quickly.
- It records all user interactions with websites or cloud-based applications.
- It accurately captures the actual user experience.
- It produces noisy data, requiring more back-end analysis.
- It lacks predictability and regularity, potentially missing problems during low utilization periods.

Synthetic transaction

- It refers to the actions performed on monitored objects in real time.
- Synthetic performance monitoring is proactive and involves external agents running scripted transactions against a web application.
- It excludes tracking of real user sessions.
- It includes tools such as Microsoft System Center Operations Manager and Foglight transaction recorder.
- Its functionalities include monitoring websites, databases, and TCP ports.

Quick Check

You want to test the performance of your e-commerce website prior to launch to find issues before the customers do and measure the impact of third-party applications on the site's performance. What test should you perform?

A. Synthetic transaction monitoring

B. Real user monitoring

C. Artificial transactions monitoring

D. Black-box test

Software Testing

Software Application

It is a computer software designed to perform a group of coordinated functions, tasks, or activities for the user’s benefit.

A software testing:

- Examines artifacts and software behavior under test by validation and verification
- Provides an objective, independent view of the software to allow the business to understand the risks of software implementation

Importance of Software Application Security

Software is a critical component in system security.

Software is the heart of the modern enterprise and performs business-critical functions.

Software failures can disrupt businesses with severe consequences.

Software applications rely on databases that also contain sensitive information.

Software applications often have privileged access to the operating system, hardware, and other resources.

Software applications routinely handle sensitive information (credit card numbers, social security numbers, and proprietary business information).

Software Assurance (SwA)

It is the level of confidence that software is free from vulnerabilities and functions in the intended manner.

The vulnerabilities could be intentionally designed into the software or accidentally inserted at any time during its lifecycle.

The main objective of SwA is to ensure that the processes, procedures, and products used to produce and sustain the software conform to all the requirements and standards.

Software Assurance Activities

Audit

Testing

Code reviews

Verification and Validation

These processes ensure that a product meets specified requirements and fulfills its intended purpose.

Verification	Validation
Evaluates if the system is implemented correctly	Evaluates if the correct system is implemented
Evaluates products during the development phase	Evaluates products at the closing of development process
Ensures the product is per requirements and design specification	Ensures the product meets user requirements
Includes activities such as reviews, meetings, and inspections	Includes activities such as black box, white box, and grey box testing
Verifies if the outputs are according to inputs or not	Validates if the users accept software or not
Evaluates plans, requirement and design specifications, code, and test cases	Evaluates actual product or software under test
Conducts manual checking of documents and files	Checks the developed products using documents and files

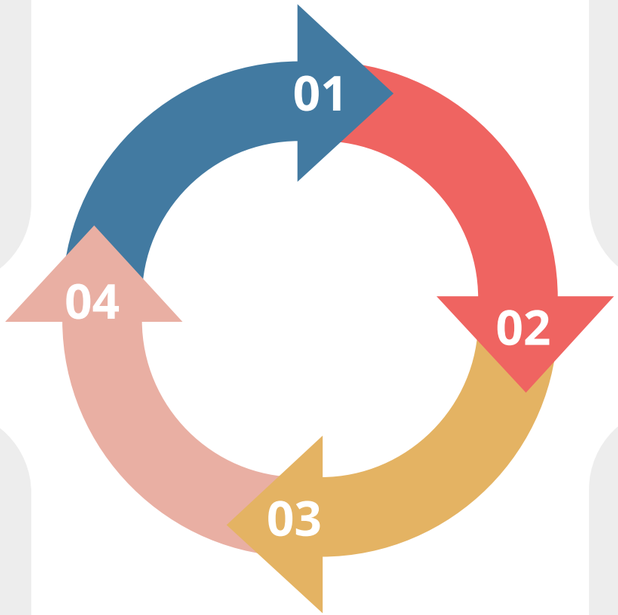
Security Testing in the SDLC

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	Or	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

Automated vs. Manual Testing

Automated testing	Manual testing
It is done using software tools that automate the examination of the code.	It is done by a skilled manual tester.
It allows the code to be reviewed quickly.	It may take a longer time and spot issues that are not evident to the one-size-fits-all automated scanner.
Disadvantage: An automated tool may miss certain issues.	**Disadvantage**: The accuracy and thoroughness of manual testing are highly dependent upon the skill of the individual reviewing the code.

Black Box vs. White Box Testing

Black box	White box
This testing is performed without any internal knowledge of the workings of the application.	This testing is performed with detailed information regarding the inner workings of the application.
Source code is not available, requiring black-box testing to be conducted by running the application itself.	Source code is often available and reviewed.
It relies on a skilled individual who can run the application and thoroughly test all aspects of the application via testing.	The in-depth review allows the tester to identify coding issues that may be less evident during a black-box test.

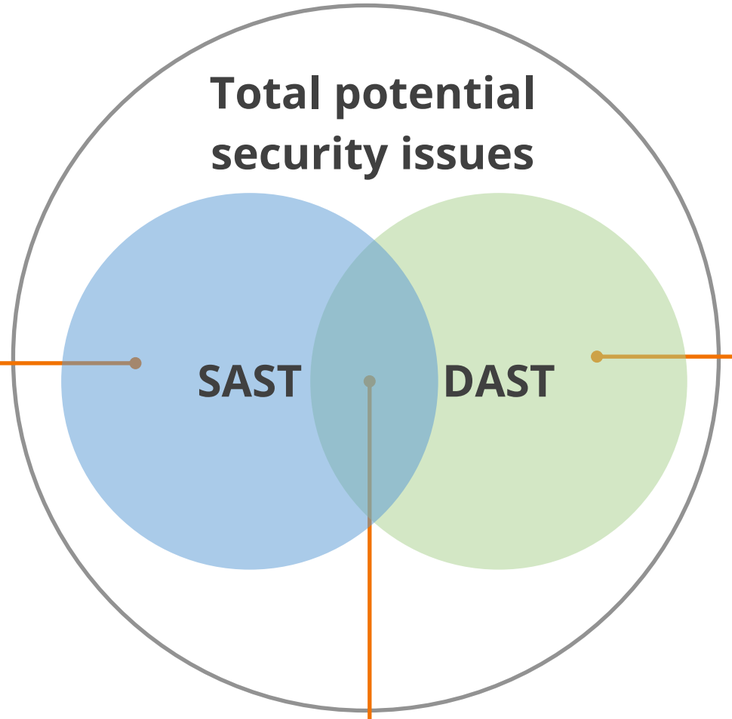
Source Code Analysis Tools

Static application security test (SAST)	Dynamic application security test (DAST)
White-box security test	Black-box security test
Requires source code	Requires a running application
Finds vulnerabilities in the earlier stages of an SDLC	Finds vulnerabilities towards the later stages of an SDLC
Is less expensive to fix vulnerabilities	Is more expensive to fix vulnerabilities
Can not discover runtime and environment related issues	Can discover runtime and environment related issues
Supports all software	Predominantly deals with web applications

SAST vs. DAST

SAST only

- Hard-coded secrets
- Code quality issues
- Issues in dead or unused code
- Insecure crypto functions
- Complex injection issues



DAST only

- Environment configuration issues
- Patch-level issues
- Runtime privilege issues
- Authentication issues
- Session management issues

DAST and SAST

- SQL injection
- Cross-site scripting
- Buffer overflows
- Path traversal
- Format string issues

IAST and RASP

The following are advanced security techniques that monitor applications in real-time:

Interactive application security testing (IAST)

- Combines the advantages of SAST and DAST
- Agents and sensors within an application analyze all interactions to identify vulnerabilities in real time.
- Accurately identifies the source of vulnerability
- Performed during the early stages of the SDLC
- Integrates easily into CI/CD pipelines

Runtime application security protection (RASP)

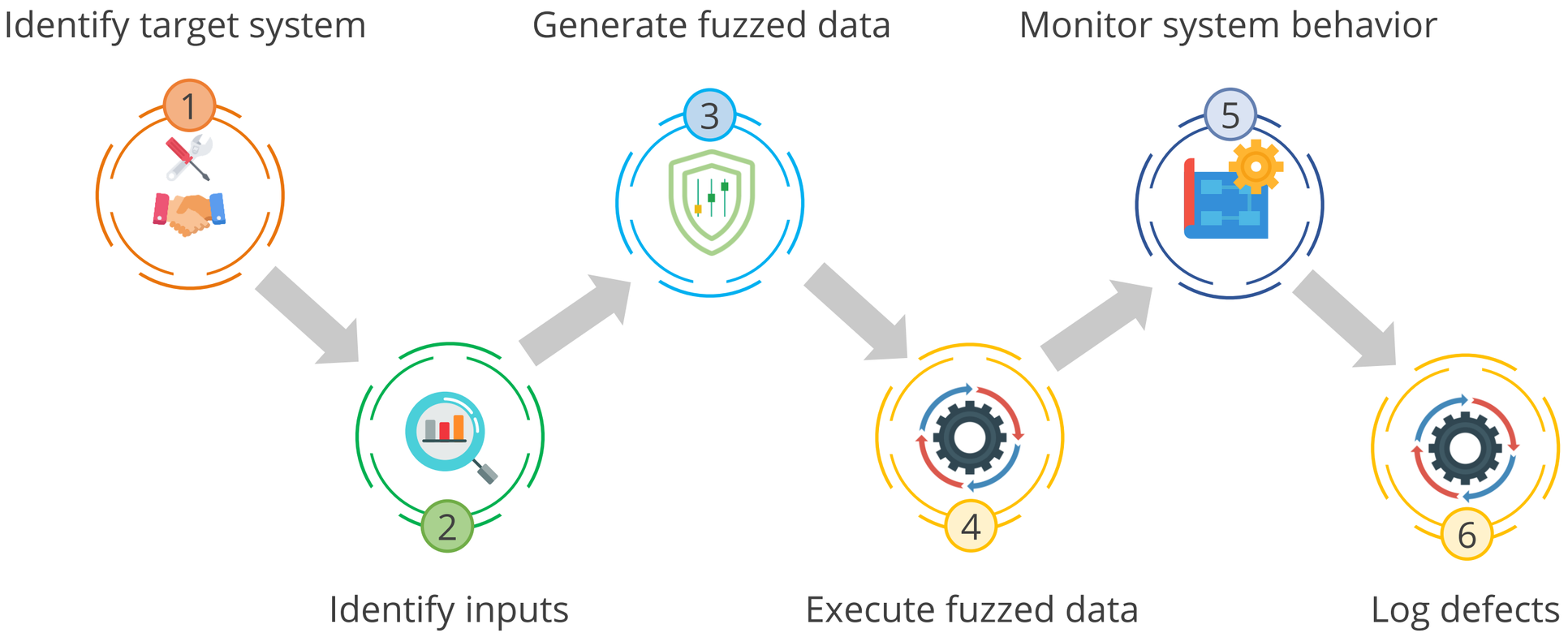
- Incorporates security into a running application on a server
- Detects and blocks cyber attacks on an application in real time without human intervention
- May have an adverse effect on application performance
- May create a sense of false security within a development team

Dynamic Fuzzing

It is an automated software testing method that injects invalid, malformed, or unexpected inputs into a system to reveal software defects and vulnerabilities.

It injects these inputs into the system and then monitors for exceptions such as crashes or information leakage.

Dynamic Fuzzing Process



Types of Dynamic Fuzzing

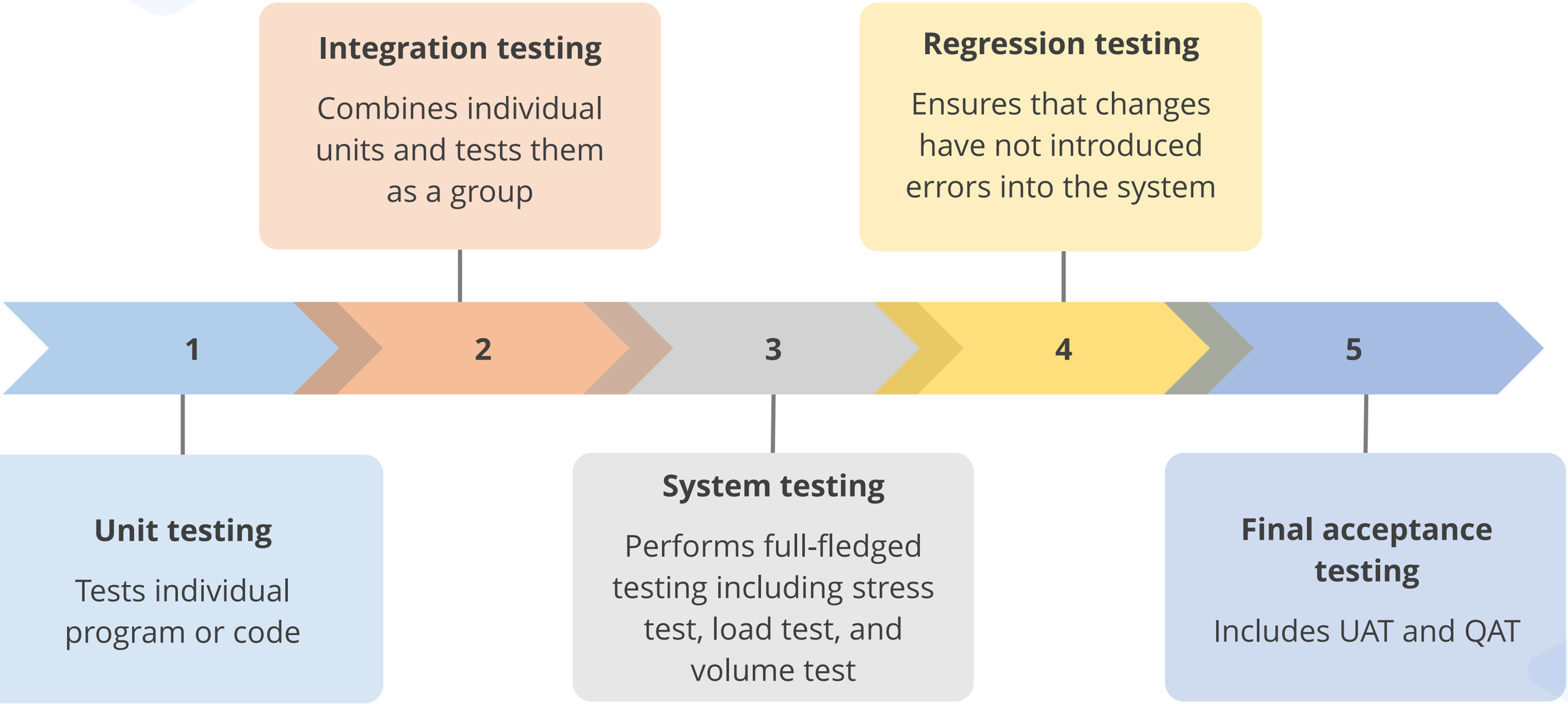
Mutation or dumb fuzzing

- Takes previous input values from the actual operation of the software and manipulates it to create fuzzed input, causing alterations
- ZZUF tool automates the process of mutation fuzzing

Generational fuzzing

- Develops data models and creates new fuzzed input based on an understanding of the types of data used by the program
- Peach fuzzing platform aids in generational fuzzing

Software Testing Levels



Unit Testing

It is a type of software testing where individual units or components of a software are tested.

- It validates that each unit of the software code performs as expected.
- It is done during the development (coding phase) of an application by the developers.

Integration Testing

It is a type of software testing where components of the software are gradually integrated and then tested as a unified group.

- These components usually work well individually but may break when integrated with other components.
- Testers want to find defects that surface due to code conflicts between software modules when they are integrated with each other.

Approaches to Integration Testing

Bottom-up approach

Testers start with individual modules at the lowest level, gradually moving to higher-level modules.

Top-down approach

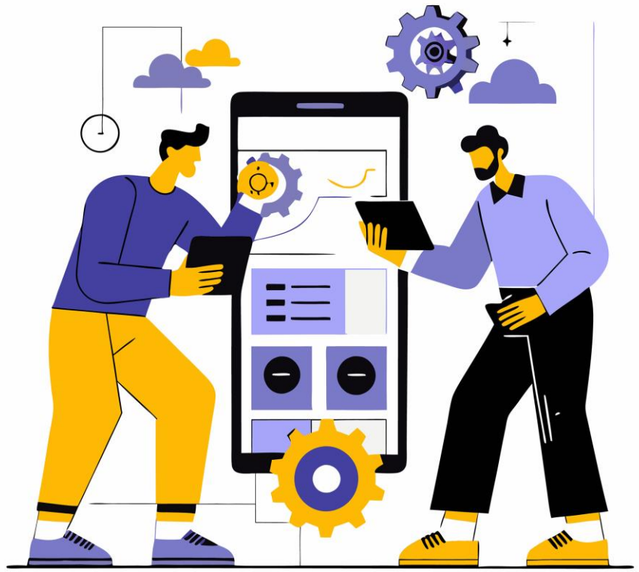
Testers start with the highest-level modules, gradually moving to lower-level modules.

Hybrid approach

Testers employ both top-down and bottom-up testing simultaneously.

Interface Testing

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

It is a part of integration testing.

Types of Interface

Application programming interface (API)

- It offers a standard way for code modules to interact and may be exposed to outside world.
- The developers test API to ensure they enforce all security requirements.

User interface (UI)

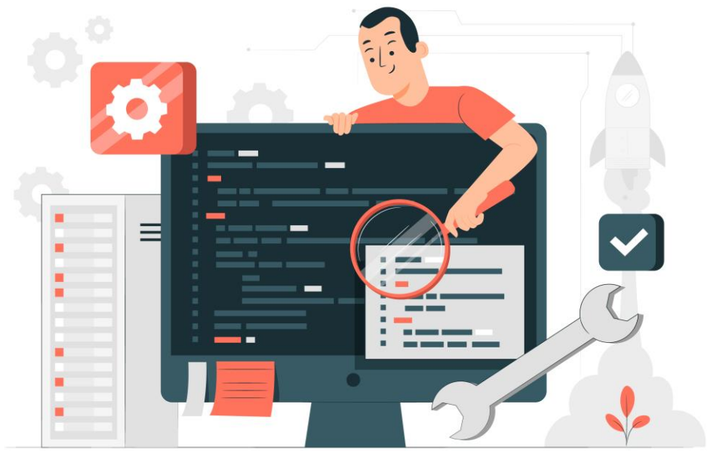
- The graphic user interface and command-line interfaces provide end-users with the ability to interact with the software.
- The test includes reviews of all UI to verify that they function properly.

Physical interface (PI)

- It exists in some applications that manipulate machinery and logic controllers.
- Testers focus diligently on PI due to the significant consequences that may arise from a failure.

System Testing

It is a level of testing that validates the complete and fully integrated software product.



- It evaluates end-to-end system specifications.
- It is a series of different tests whose sole purpose is to exercise the full computer-based system.

Types of System Tests

Functionality testing

Recoverability testing

Performance testing

Usability testing

Hardware and software testing

Types of System Tests

Functionality testing

- It determines whether the system, especially features, complies with the requirements.
- It ensures that the product's functionality complies with the specified standards while staying within the bounds of the system.

Recoverability testing

- It checks if the system can bounce back from crashes, hardware failures, and other significant issues.
- It also determines how effectively the method jumps back from different input errors and other failures.

Types of System Tests

Performance testing

- It verifies if the components of the system abide by the performance characteristics.
- It establishes if a system achieves its performance goals, such as throughput or reaction time.

Usability testing

- It examines the system’s user-friendliness to guarantee that the system is simple to understand, operate, and use.

Types of System Tests

Hardware and software testing

- It tests the hardware and software of a system.
- It examines the functionality of each piece of hardware and software to ensure that it functions as intended.

Regression Testing

It is a type of software testing to confirm that a recent program or code change has not adversely affected the existing features.

- It is a full or partial selection of already executed test cases that are re-executed to ensure existing functionalities work fine.
- It ensures that the old code works even after the latest code changes are done.

Final Acceptance Testing

It is a testing technique that determines whether the software system meets the requirement specifications.

It evaluates the system's compliance with the business requirements and verifies if it has met the required criteria for delivery to end users.

Types of Acceptance Tests

User acceptance test

Determines if the product is working as intended for the user

Business acceptance testing

Determines if the product meets the business goals and purposes

Alpha testing

Assesses the product in the development testing environment by a specialized testers team, called alpha testers

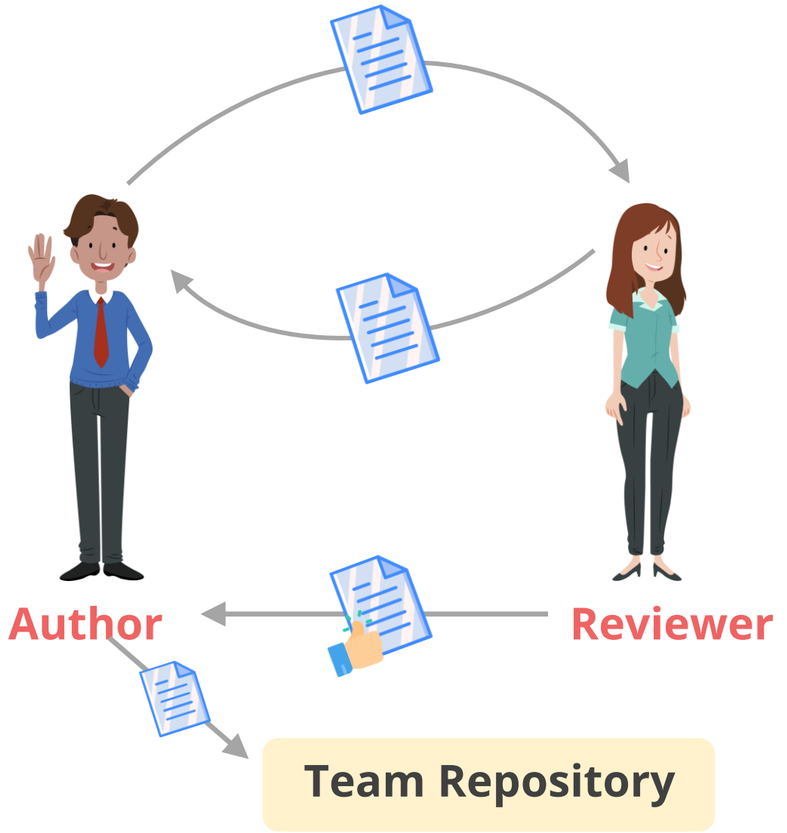
Beta testing

Assesses the product by exposing it to the real end-users in their environment, called beta testers

Code Review

It is a systematic examination of instructions that comprise a piece of software performed by someone other than the author of that code.

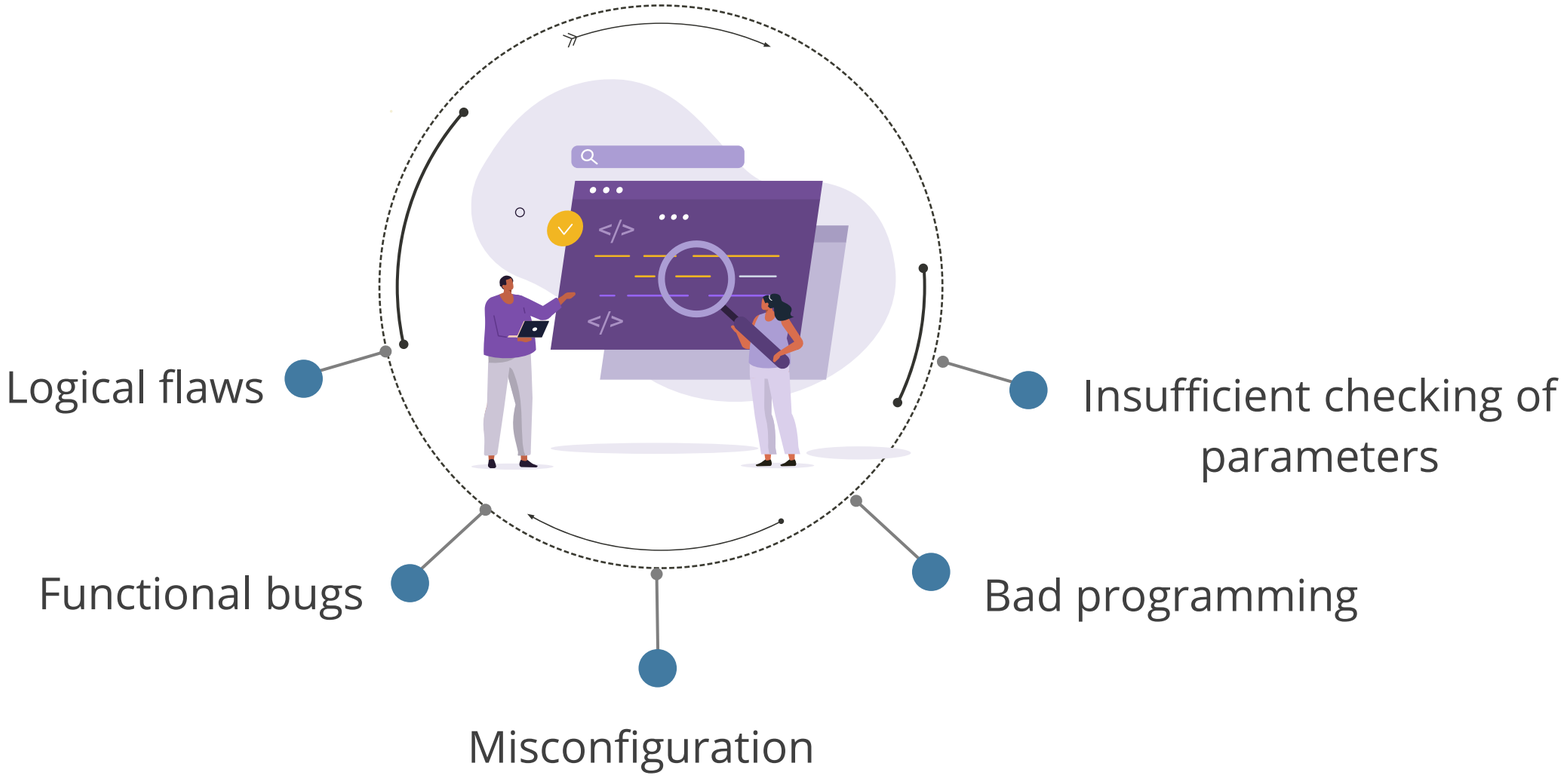
- It is also called peer review and is the foundation of software assessment programs.
- It starts with the organization setting the coding standards to be followed.
- The primary step is to ensure the developer follows the defined coding standard.
- After that, the reviewer checks for functions that are not needed or procedures that may lead to code bloat.



Security must be included in all the phases of the software development life cycle (SDLC) since a coding error can make a system vulnerable and compromise its security.

Code Review

Software vulnerabilities are mainly caused by:



Types of Code Review

Pair programming

- It is an agile software development technique that places two developers at one workstation where one developer writes the code, while the other reviews it.
- Frequent role switches ensure that both developers are coding and reviewing equally and are familiar with all the code.

Pass around code

- It works by sending code to reviewers who check the code later.
- It is less time-intensive than pair or over-the-shoulder reviews, but it also means that developers do not receive immediate feedback.

Types of Code Review

Over the shoulder

It requires one developer to write the code while the other watches and reviews the code.

Tool assisted review

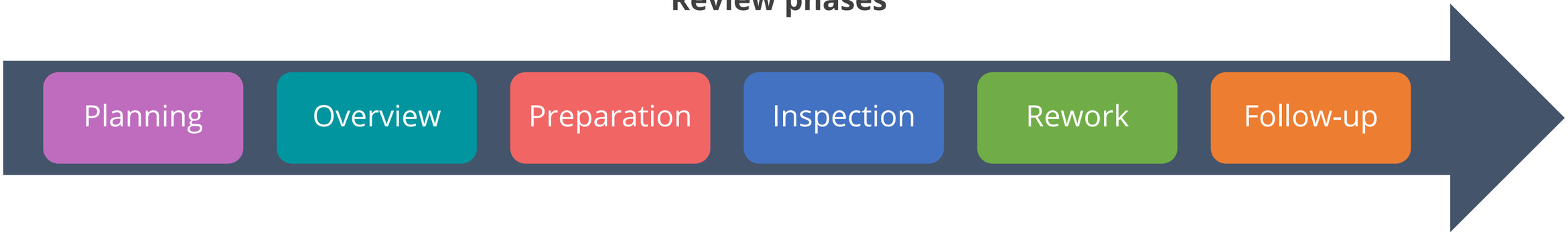
It relies on a formal or informal tool to ensure that code is reviewed and receives proper sign-off.

Fagan Code Review Process

It tries 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 as the inventor of formal software inspections.

Review phases

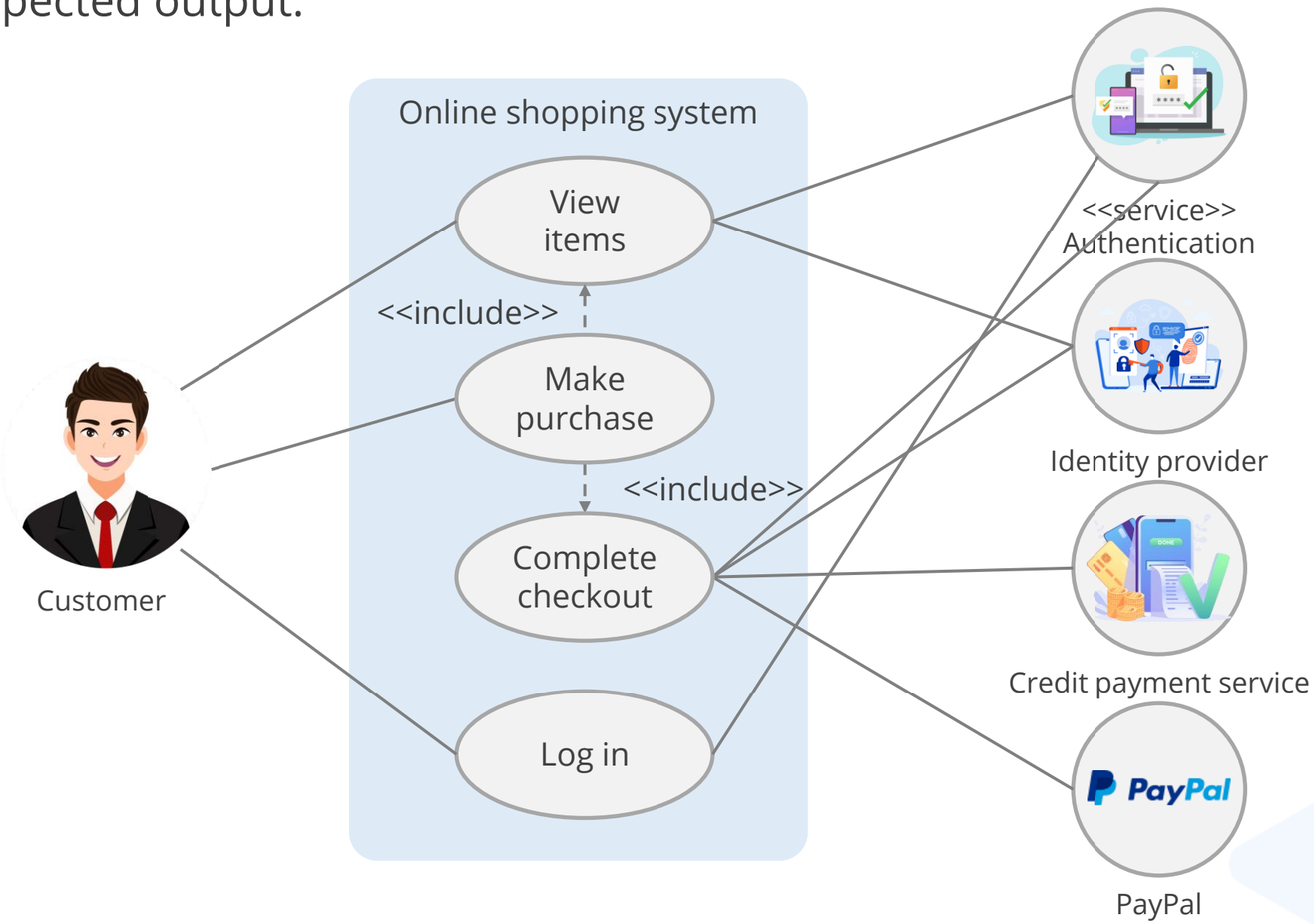


This level of formality is normally found only in highly restrictive environments where code flaws may have a catastrophic impact.

Use Case or Positive Testing

It describes the sequence of actions between the user and the system that result in an expected output.

- They are textual but are graphically represented using the unified modeling language (UML).
- They are related to one another in different ways called associations.
- They are helpful in determining the normal or expected behavior of a system rather than in assessing its security.



Misuse or Abuse Case Testing

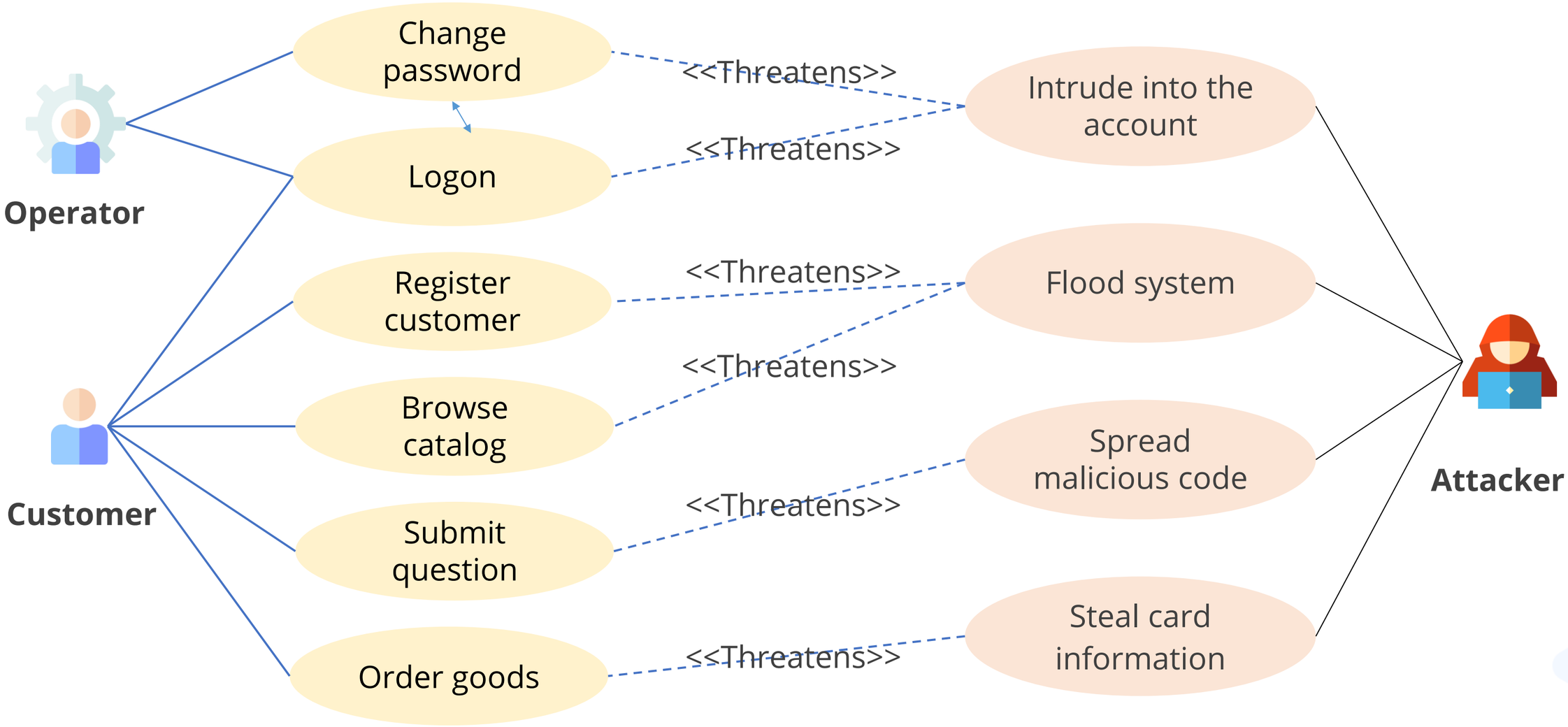
It focuses on threat actors and the actions they want to perform on a system.

- 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.
- This testing helps to ensure one has effectively addressed each of the risks identified and has decided to mitigate them during the risk assessment phase.
- It doesn’t require including all the possible threats to the system, but it should include the ones that have to be addressed.
- It is used by software developers to evaluate the vulnerability of their software to risks.

Use Case vs. Misuse Case

Positive testing	Abuse testing
It verifies the system using valid input data.	It verifies the system against invalid input data.
It is done to test whether the application works as expected.	It is done to detect situations like unexpected user behavior or invalid input and prevent applications from crashing.
It fails if an error is encountered during testing.	It aims at finding an application’s weak points, thus helping improve its quality.

Use Case vs. Misuse Case



Test Coverage Analysis

It 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, also called 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 = Number of use cases tested or total number of use cases
- This is a highly subjective calculation.

Code Coverage Analysis

It refers to how well the test set is covering the source code.

Different functionalities to be tested during code coverage include:

- **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 all subsequent if-else body
- **Loop coverage**: Every possible loop to be executed one time, more than once, and zero times
- **Entry and exit coverage**: All possible calls and their return value

Breach Attack Simulations (BAS)

Gartner defines 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.

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

Key capabilities and functions:

- 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
- Includes recommendations for mitigation in comprehensive reports

Compliance Checks

It is the review and analysis of the implemented controls to check whether they follow regulations, laws, and policies.

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

Quick Check

You want to ensure that the newly added features of the software do not negatively impact the already existing features of the software. Which test should you perform?

A. System integration test

B. Regression test

C. Fuzz test

D. User acceptance test

Quick Check

You need to ensure that the components of your e-commerce website are working correctly. You intend to verify the APIs, web services, error handling, and session management capabilities of the website. What type of test should you conduct?

A. Unit test

B. Interface test

C. Regression test

D. Fuzz test

Account Management and Performance Measurement

Account Management

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

The data collection also includes verification of the account provisioning process and the accounts' privileges.

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

Account Management

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

Deprovisioning includes:

- Access removal when an employee leaves the company
- Account adjustments during change in designations
- Review of 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 Indicator (KPI)

It is a metric used to measure the effectiveness and performance of security controls and processes.

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

- An actual value of a factor at a particular point in time
- **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:** AV alerts per month will not be more than 25 or 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
- **Example:** Percentage of valid alerts compared to total AV alerts, indicating the quality of threat detection

KPI Process

- Choose the factors that can show the state of security
- Define baselines for some or all factors under consideration
- Develop a plan for periodically capturing the values of these factors
- Analyze and interpret the data
- Communicate the indicators to all stakeholders

Key Risk Indicator (KRI)

It indicates where an organization is in relation to its risk appetite.

- It measures how risky an activity is so that leadership can make informed decisions about it.
- It is selected for its impact on the decisions of the senior leaders in an organization.
- It must relate to SLE equations.
- It alerts the organization when an unfavorable situation might arise, allowing them to plan for these situations.

Key Performance and Risk Indicators

Key performance indicator (KPI)

- They measure how well something is being done.
- They can be parameters such as cost adherence, schedule adherence, and project effort adherence.

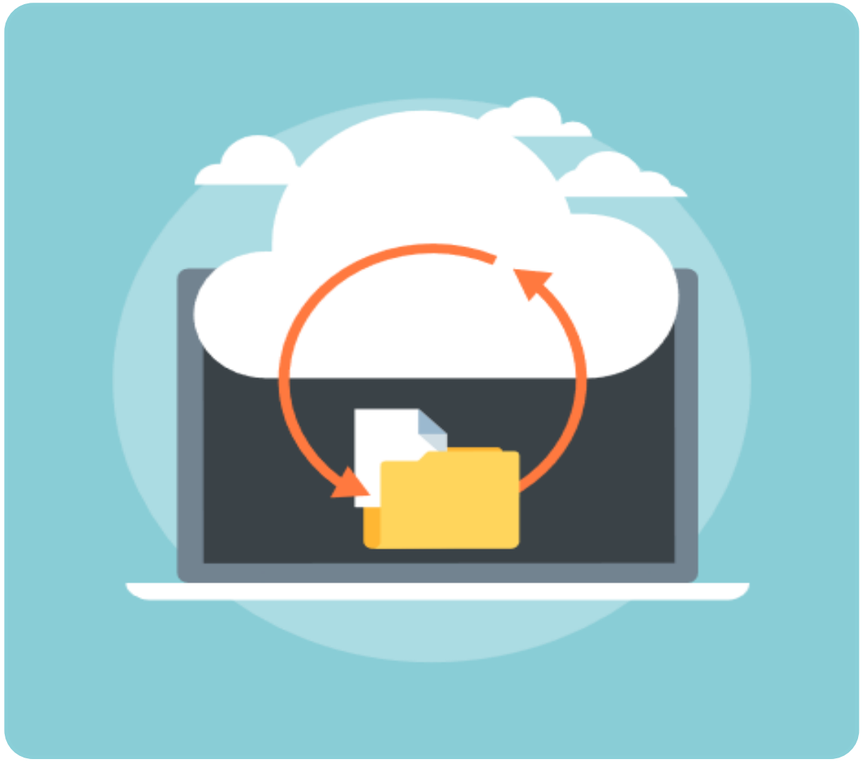
Key risk indicator (KRI)

- They indicate how risky an activity is or the possibility of an adverse impact in the future.
- They 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 refers to the information and processes used to confirm the integrity, accuracy, and completeness of data backups.

- 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)

It is the process of informing employees about security best practices.

- It reduces risks by addressing the behavioral element of security through education and consistent application of awareness techniques.
- It focuses on common user security concerns such as password selection, appropriate use of computing resources, and social engineering attacks.
- It is tailored to the target audience.

Quick Check

As an IT manager ensuring that your organization's backup verification processes are reliable and thorough, which of the following practices is most important for maintaining data integrity?

A. Scheduling backups during off-peak hours
B. Using high-quality storage media
C. Regularly testing stored data to verify integrity
D. Increasing the frequency of backups

Ethical Disclosure of Information

Ethical Disclosure

It promotes trust by sharing relevant information.

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 to enable organizations at risk to 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.

Quick Check

A security consultant identifies a critical vulnerability in a client's system during a penetration test that could expose sensitive customer data. What should the consultant do next?

A. Exploit the vulnerability to demonstrate the risk to the client’s executives

B. Inform the client immediately of the vulnerability and provide recommendations for remediation

C. Report the vulnerability to external regulatory authorities to ensure transparency

D. Ignore the vulnerability since it’s not within the original scope of the penetration test

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.
- SOC reports are a series of accounting standards that measure the control of financial information for a service organization.
- Vulnerability assessment is the process in which vulnerabilities in IT are identified and their risks evaluated.
- Penetration testing is the practice of testing a computer system, network, or web application to find security vulnerabilities that an attacker could exploit.
- The software testing level includes unit testing, integration testing, system testing, regression testing, and acceptance testing.

Thank You