Module–2(Manual Testing)

1) What is Exploratory Testing?

**exploratory Testing** is a type of software testing where Test cases are not created in advance but testers check system on the fly. They may note down ideas about what to test before test execution. The focus of exploratory testing is more on testing as a “thinking” activity.

Exploratory Testing is widely used in Agile models and is all about discovery, investigation, and learning. It emphasizes personal freedom and responsibility of the individual tester.

2)What is traceability matrix?

A Traceability Matrix is a document that co-relates any two-baseline documents that require a many-to-many relationship to check the completeness of the relationship.It is used to track the requirements and to check the current project requirements are met.

3) What is Boundary value testing?

Boundary testing is a black-box testing technique that software developers often use to check the errors at the boundaries or extreme ends of a given input domain. An input domain comprises all the possible inputs available in a software program. Software developers utilize black-box testing to analyze the behavior of a software program and examine its functionality. The extreme ends in boundary testing might include start to end, lower to upper or minimum to maximum. Instead of focusing only on the center of the data, boundary testing helps detect errors occurring at the boundary values of valid or invalid partitions.

4) What is Equivalence partitioning testing?

Equivalence Partitioning also called as equivalence class partitioning. It is abbreviated as ECP. It is a software testing technique that divides the input test data of the application under test into each partition at least once of equivalent data from which test cases can be derived. An advantage of this approach is it reduces the time required for performing testing of a software due to less number of test cases.

5)What is Integration testing?

**integration Testing** is defined as a type of testing where software modules are integrated logically and tested as a group. A typical software project consists of multiple software modules, coded by different programmers. The purpose of this level of testing is to expose defects in the interaction between these software modules when they are integrated

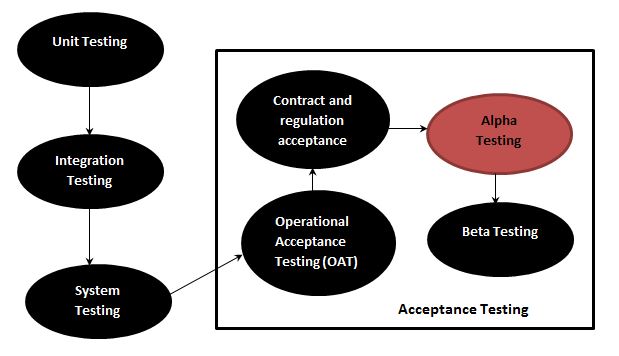
6)What determines the level of risk?

We often see situations where we have applied the best [**testing techniques**](https://www.toolsqa.com/software-testing/istqb/testing-techniques/) and processes, and yet the testing wasn't completed in time or with quality. It happens when we have not planned for risks in our testing process. In this tutorial, we will get a good understanding of Risks and it's various levels. We will also discuss how we can categorize risk in software testing basis their probability and impact.

7)What is Alpha testing?

Alpha Testing is a type of software testing performed to identify bugs before releasing the software product to the real users or public. It is a type of [acceptance testing.](https://www.guru99.com/user-acceptance-testing.html) The main objective of alpha testing is to refine the software product by finding and fixing the bugs that were not discovered through previous tests.

The following diagram explains the fitment of Alpha testing in the software development life cycle.



8)What is beta testing?

**Beta Testing** is performed by real users of the software application in a real environment. Beta testing is one of the types of **User Acceptance Testing**. A Beta version of the software, whose feedback is needed, is released to a limited number of end-users of the product to obtain feedback on the product quality. Beta testing helps in minimization of product failure risks and it provides increased quality of the product through customer validation. It is the last test before shipping a product to the customers. One of the major advantages of beta testing is direct feedback from customers.

9)What is component testing?

Component testing is defined as a software testing type, in which the testing is performed on each individual component separately without integrating with other components. It’s also referred to as Module Testing when it is viewed from an architecture perspective. Component Testing is also referred to as Unit Testing, Program Testing or Module Testing Generally, any software as a whole is made of several components. Component Level Testing deals with testing these components individually.

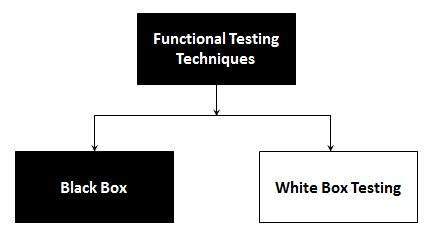
10)What is functional system testing?

Functional Testing is a type of [Software Testing](https://www.geeksforgeeks.org/software-testing-basics/) in which the system is tested against the functional requirements and specifications. Functional testing ensures that the requirements or specifications are properly satisfied by the application. This type of testing is particularly concerned with the result of processing. It focuses on simulation of actual system usage but does not develop any system structure assumptions.

It is basically defined as a type of testing which verifies that each function of the software application works in conformance with the requirement and specification. This testing is not concerned about the source code of the application. Each functionality of the software application is tested by providing appropriate test input, expecting the output and comparing the actual output with the expected output. This testing focuses on checking of user interface, APIs, database, security, client or server application and functionality of the Application Under Test.

Functional Testing Techniques:

There are two major Functional Testing techniques as shown below:



The other major Functional Testing techniques include:

* Unit Testing
* Integration Testing
* Smoke Testing
* User Acceptance Testing
* Localization Testing
* Interface Testing
* Usability Testing
* System Testing
* Regression Testing
* Globalization Testing

11)What is Non-Functional Testing?

Non-functional testing is a type of software testing to test non-functional parameters such as reliability, load test, performance and accountability of the software. The primary purpose of non-functional testing is to test the reading speed of the software system as per non-functional parameters. The parameters of non-functional testing are never tested before the functional testing. Non-functional testing is also very important as functional testing because it plays a crucial role in customer satisfaction

Types of Non Functional Testing

* Performance Tests.
* Load Tests.
* Stress Tests.
* Volume Tests.
* Security Tests.
* Upgrade & Installation Tests.
* Recovery Tests.

12) What is GUI Testing?

GUI Testing is a software testing type that checks the Graphical User Interface of the Software. The purpose of Graphical User Interface (GUI) Testing is to ensure the functionalities of software application work as per specifications by checking screens and controls like menus, buttons, icons, etc. GUI is what the user sees what you will see say homepage it is the GUI (graphical user interface) of the site. A user does not see the source code. The interface is visible to the user. Especially the focus is on the design structure, images that they are working properly or not.

13)What is Adhoc testing?

Adhoc testing is a type of software testing which is performed informally and randomly after the formal testing is completed to find out any loophole in the system. For this reason, it is also known as Random testing or Monkey testing. Adhoc testing is not performed in an structured way so it is not based on any methodological approach. That’s why Adhoc testing is a type of Unstructured Software Testing.

**Types of Adhoc Testing :**

Adhoc testing is divided into three types as follows. 

1. **Buddy Testing –**   
   Buddy testing is a type of Adhoc testing where two bodies will be involved one is from Developer team and one from tester team. So that after completing one module and after completing [Unit testing](https://www.geeksforgeeks.org/unit-testing-software-testing/) the tester can test by giving random inputs and the developer can fix the issues too early based on the currently designed test cases.

1. **Pair Testing –**   
   Pair testing is a type of Adhoc testing where two bodies from the testing team can be involved to test the same module. When one tester can perform the random test and another tester can maintain the record of findings. So when two testers get paired they exchange their ideas, opinions and knowledge so good testing is performed on the module.

1. **Monkey Testing –**   
   Monkey testing is a type of Adhoc testing in which the system is tested based on random inputs without any test cases and the behavior of the system is tracked and all the functionalities of the system is working or not is monitored. As the randomness approach is followed there is no constraint on inputs so it is called as Monkey testing.

14)What is load testing?

**Load Testing** is a type of [Performance Testing](https://www.geeksforgeeks.org/performance-testing-software-testing/) that determines the performance of a system, software product, or software application under real-life based load conditions. Basically, load testing determines the behavior of the application when multiple users use it at the same time. It is the response of the system measured under varying load conditions. The load testing is carried out for normal and extreme load conditions.

Load testing is a type of performance testing that simulates a real-world load on a system or application to see how it performs under stress. The goal of load testing is to identify bottlenecks and determine the maximum number of users or transactions the system can handle. It is an important aspect of software testing as it helps ensure that the system can handle the expected usage levels and identify any potential issues before the system is deployed to production.

16)What is stress Testing?

**Stress Testing** is a software testing technique that determines the robustness of software by testing beyond the limits of normal operation. Stress testing is particularly important for critical software but is used for all types of software. Stress testing emphasizes robustness, availability, and error handling under a heavy load rather than what is correct behavior under normal situations. Stress testing is defined as a type of software testing that verifies the stability and reliability of the system. This test particularly determines the system on its robustness and error handling under extremely heavy load conditions. It even tests beyond the normal operating point and analyses how the system works under extreme conditions. Stress testing is performed to ensure that the system would not crash under crunch situations.

17)What is white box testing and list the types of white box testing?

**White Box Testing** is a testing technique in which software’s internal structure, design, and coding are tested to verify input-output flow and improve design, usability, and security. In white box testing, code is visible to testers, so it is also called Clear box testing, Open box testing, Transparent box testing, Code-based testing, and Glass box testing.

It is one of two parts of the Box Testing approach to software testing. Its counterpart, Blackbox testing, involves testing from an external or end-user perspective. On the other hand, White box testing in software engineering is based on the inner workings of an application and revolves around internal testing.

Types of white box testing?

* **Unit Testing:** It is often the first type of testing done on an application.[Unit Testing](https://www.guru99.com/unit-testing-guide.html) is performed on each unit or block of code as it is developed. Unit Testing is essentially done by the programmer. As a software developer, you develop a few lines of code, a single function or an object and test it to make sure it works before continuing Unit Testing helps identify a majority of bugs, early in the software development lifecycle. Bugs identified in this stage are cheaper and easy to fix.
* **Testing for Memory Leaks**: Memory leaks are leading causes of slower running applications. A QA specialist who is experienced at detecting memory leaks is essential in cases where you have a slow running software application.

18)What is black box testing? What are the different black box testing techniques?

**Black Box Testing** is a software testing method in which the functionalities of software applications are tested without having knowledge of internal code structure, implementation details and internal paths. Black Box Testing mainly focuses on input and output of software applications and it is entirely based on software requirements and specifications. It is also known as Behavioral Testing.

What are the different black box testing techniques?

* **Equivalence Class Testing:** It is used to minimize the number of possible test cases to an optimum level while maintains reasonable test coverage.
* **Boundary Value Testing:** Boundary value testing is focused on the values at boundaries. This technique determines whether a certain range of values are acceptable by the system or not. It is very useful in reducing the number of test cases. It is most suitable for the systems where an input is within certain ranges.
* **Decision Table Testing**: A decision table puts causes and their effects in a matrix. There is a unique combination in each column.

19)Mention what are the categories of defects?

A software bug arises when the expected result doesn’t match with the actual results. It can also be error, flaw, failure, or fault in a computer program. Most bugs arise from mistakes and errors made by developers, architects.

Following are the methods for preventing programmers from introducing bugs during development:

* Programming Techniques adopted
* Software Development methodologies
* Peer Review
* Code Analysis

## Common Types of Defects

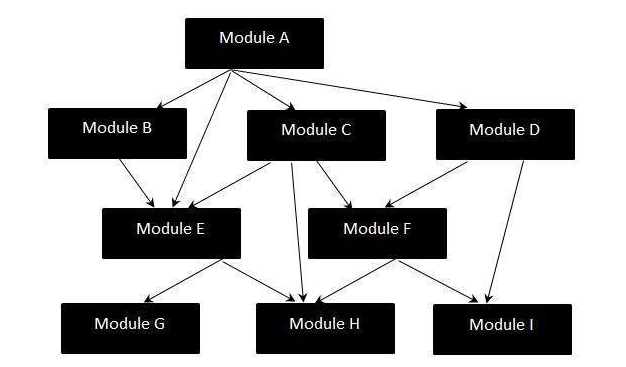
Following are the common types of defects that occur during development:

* Arithmetic Defects
* Logical Defects
* Syntax Defects
* Multithreading Defects
* Interface Defects
* Performance Defects

**20)**Mention what bigbang testing is?

* Big Bang Integration Testing is an integration testing strategy wherein all units are linked at once, resulting in a complete system. When this type of testing strategy is adopted, it is difficult to isolate any errors found, because attention is not paid to verifying the interfaces across individual units.

## Big Bang Integration – Work Flow Diagram

Big Bang Testing is represented by the following workflow diagram:

## Disadvantages of Big-Bang Testing

* Defects present at the interfaces of components are identified at very late stage as all components are integrated in one shot.
* It is very difficult to isolate the defects found.
* There is high probability of missing some critical defects, which might pop up in the production environment.
* It is very difficult to cover all the cases for integration testing without missing even a single scenario.

21) What is the purpose of exit criteria?

Exit criterion is used to determine whether a given test activity has been completed or NOT. Exit criteria can be defined for all of the test activities right from planning, specification and execution.

Exit criterion should be part of test plan and decided in the planning stage.

## Examples of Exit Criteria:

* Verify if All tests planned have been run.
* Verify if the level of requirement coverage has been met.
* Verify if there are NO Critical or high severity defects that are left outstanding.
* Verify if all high risk areas are completely tested.
* Verify if software development activities are completed within the projected cost.
* Verify if software development activities are completed within the projected timelines.

22)When should "Regression Testing" be performed?

Regression testing is a black box testing techniques. It is used to authenticate a code change in the software does not impact the existing functionality of the product. Regression testing is making sure that the product works fine with new functionality, [bug](https://www.javatpoint.com/bug-in-software-testing) fixes, or any change in the existing feature.

Regression testing is a type of [software testing](https://www.javatpoint.com/software-testing-tutorial). Test cases are re-executed to check the previous functionality of the application is working fine, and the new changes have not produced any bugs.

Regression testing can be performed on a new build when there is a significant change in the original functionality. It ensures that the code still works even when the changes are occurring. Regression means Re-test those parts of the application, which are unchanged.

Regression tests are also known as the Verification Method. Test cases are often automated. [Test cases](https://www.javatpoint.com/test-case) are required to execute many times and running the same test case again and again manually, is time-consuming and tedious too.

23)What is 7 key principles? Explain in detail?

There are **seven fundamental testing principles** which help the testing teams to utilize their time and effort and make the testing process an effective one.

* [Testing shows presence of defects](https://www.edureka.co/blog/seven-principles-of-software-testing/#testingdefects)
* [Exhaustive Testing is not possible](https://www.edureka.co/blog/seven-principles-of-software-testing/#exhaustivetesting)
* [Early Testing](https://www.edureka.co/blog/seven-principles-of-software-testing/#earlytesting)
* [Defect Clustering](https://www.edureka.co/blog/seven-principles-of-software-testing/#defectclustering)
* [Pesticide Paradox](https://www.edureka.co/blog/seven-principles-of-software-testing/#pesticideparadox)
* [Testing is context-dependent](https://www.edureka.co/blog/seven-principles-of-software-testing/#contextdependent)
* [Absence of errors fallacy](https://www.edureka.co/blog/seven-principles-of-software-testing/#errorfallacy)

**1. Testing shows presence of defects**

* Testing an application is important to know whether any **error or defect exists**. The objective is to find more and more hidden defects using different techniques and methods. Testing helps you reveal undiscovered defects and if no defects are found then it does not mean that the **software** is **defect-free**.
* For example, an application might seem to be error-free after going through different stages of testing. But during the production in the environment, the user may come across any defect which did not occur during the testing.

### **2. Exhaustive testing is not possible**

* It is difficult to test all the functionalities with valid and invalid combinations of input data during actual testing. Therefore, testing of a few combinations is done based on priority using different techniques.**Exhaustive testing** will take **unlimited efforts** and most of those efforts are ineffective. Also, the project timelines would not allow testing of so many combinations.
* For example, If you have an input field which accepts alphabets, special characters, and numbers from 0 to 1000 only, it would have numerous combinations for testing. It is not possible to test all combinations for each input type

. **3. Early testing.**

Testers get involved in the early stage to find defects during the**requirement analysis phase**. The cost involved in fixing such defects is very less when compared to those that are found during the later stages of testing.

Testing needs to be performed on requirement documents, specification or any other type of document so that if requirements are incorrectly defined then it can be**fixed immediately** rather than fixing them in the **development phase**.

### **4. Defect clustering**

During testing, it is observed that most of the **defects** found are related to a small number of **modules**. There might be multiple reasons for this like the modules may be complex, coding related to such modules may be complicated, etc.

This is the Pareto Principle of software testing where you can detect 80% of the problems in 20% of the modules.

### **5. Pesticide paradox**

Pesticide Paradox principle states that if you execute the same set of test cases again and again over the period of time then these set of tests cannot identify new defects in the system.

In order to overcome this **Pesticide Paradox**, you need to review and revise the set of test cases regularly. If required a new set of test cases can be added. and the existing test cases can be deleted if they are not able to find any more defects from the system.

### **6. Testing is context-dependent**

There are various domains available in the market and each domain has a number of applications. For each domain, their applications have different requirements, functions, different testing purpose, risk, techniques, etc. Different domains are tested differently and thus the testing is purely based on the **context** of the **domain** or application.

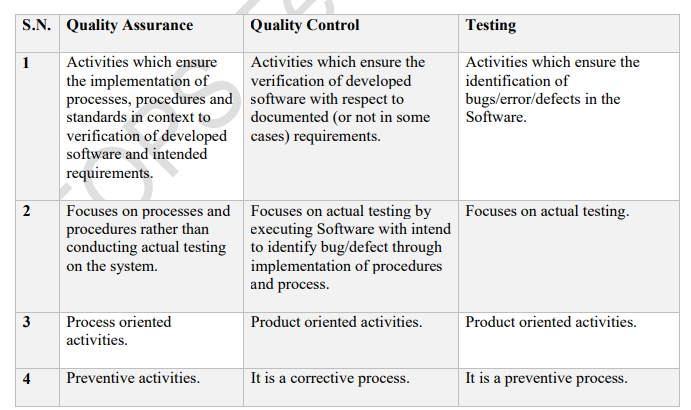
For Example, testing a banking application is different than testing any e-commerce or advertising application. The risk associated with each type of application is different. So, you should not use the same method, technique, and testing type to test different applications.

### **7. Absence of errors fallacy**

If the software is tested fully and no defects are found before release, then you can consider the software to be 99% defect-free. But if the software is tested against **wrong requirements**, finding defects and fixing them on time would not help as testing is performed on wrong requirements. This would not comply with the user needs.

For Example, suppose you are testing an application related to an e-commerce site and the requirements against “Shopping Cart or Shopping Basket” functionality is wrongly interpreted and tested. Here, finding moredefects would not help you in moving the application into the next phase or in the production environment.

24)Difference between QA v/s QC v/s Tester



25)Difference between Smoke and Sanity?

#### Smoke Testing has a goal to verify “stability” whereas Sanity Testing has a goal to verify “rationality”.

* Smoke Testing is done by both developers or testers whereas Sanity Testing is done by testers.
* Smoke Testing verifies the critical functionalities of the system whereas Sanity Testing verifies the new functionality like bug fixes.
* Smoke testing is a subset of acceptance testing whereas Sanity testing is a subset of Regression Testing.
* Smoke testing is documented or scripted whereas Sanity testing isn’t.
* Smoke testing verifies the entire system from end to end whereas Sanity Testing verifies only a particular component.

26) Difference between verification and Validation

| Verification | Validation |
| --- | --- |
| It includes checking documents, design, codes and programs. | It includes testing and validating the actual product. |
| Verification is the static testing. | Validation is the dynamic testing. |
| It does not include the execution of the code. | It includes the execution of the code. |
| Methods used in verification are reviews, walkthroughs, inspections and desk-checking. | Methods used in validation are Black Box Testing, White Box Testing and non-functional testing. |
| It checks whether the software conforms to specifications or not. | It checks whether the software meets the requirements and expectations of a customer or not. |
| It can find the bugs in the early stage of the development. | It can only find the bugs that could not be found by the verification process. |
| The goal of verification is application and software architecture and specification. | The goal of validation is an actual product. |
| Quality assurance team does verification. | Validation is executed on software code with the help of testing team. |
| It comes before validation. | It comes after verification. |
| It consists of checking of documents/files and is performed by human. | It consists of execution of program and is performed by computer. |

27) **Explain types of Performance testing.**

Performance testing, a non-functional testing technique performed to determine the system parameters in terms of responsiveness and stability under various workload. Performance testing measures the quality attributes of the system, such as scalability, reliability and resource usage.

## Performance Testing Techniques:

* **Load testing -**It is the simplest form of testing conducted to understand the behaviour of the system under a specific load. Load testing will result in measuring important business critical transactions and load on the database, application server, etc., are also monitored.
* **Stress testing -**It is performed to find the upper limit capacity of the system and also to determine how the system performs if the current load goes well above the expected maximum.
* **Soak testing -**Soak Testing also known as endurance testing, is performed to determine the system parameters under continuous expected load. During soak tests the parameters such as memory utilization is monitored to detect memory leaks or other performance issues. The main aim is to discover the system's performance under sustained use.
* **Spike testing -**Spike testing is performed by increasing the number of users suddenly by a very large amount and measuring the performance of the system. The main aim is to determine whether the system will be able to sustain the workload.

28) What is Error, Defect, Bug and failure?

“A mistake in coding is called error, error found by tester is called defect, defect accepted by development team then it is called bug, build does not meet the requirements then it is failure”

Error: A discrepancy between a computed, observed, or measured value or condition and the true, specified, or theoretically correct value or condition. This can be a misunderstanding of the internal state of the software, an oversight in terms of memory management, confusion about the proper way to calculate a value, etc.

Failure: The inability of a system or component to perform its required functions within specified performance requirements. See: bug, crash, exception, and fault.

Bug: A fault in a program which causes the program to perform in an unintended or unanticipated manner. See: anomaly, defect, error, exception, and fault. Bug is terminology of Tester.

Defect: Commonly refers to several troubles with the software products, with its external behavior or with its internal features.

29) Difference between Priority and Severity

| Severity | Priority |
| --- | --- |
| Severity is a parameter to denote the impact of a particular defect on the software. | Priority is a parameter to decide the order in which defects should be fixed. |
| Severity means how severe defect is affecting the functionality. | Priority means how fast defect has to be fixed. |
| Severity is related to the quality standard. | Priority is related to scheduling to resolve the problem. |
| Testing engineer decides the severity level of the defect. | Product manager decides the priorities of defects. |
| Its value is objective. | Its value is subjective. |
| Its value doesn’t change from time to time. | Its value changes from time to time. |
| Severity is of 5 types: Critical, Major, Moderate, Minor, and Cosmetic. | Priority is of 3 types: Low, Medium, and High. |

30) What is Bug Life Cycle?

## Workflow:

## 

## Defect Life Cycle States:

* New - Potential defect that is raised and yet to be validated.
* Assigned - Assigned against a development team to address it but not yet resolved.
* Active - The Defect is being addressed by the developer and investigation is under progress. At this stage there are two possible outcomes; viz - Deferred or Rejected.
* Test - The Defect is fixed and ready for testing.
* Verified - The Defect that is retested and the test has been verified by QA.
* Closed - The final state of the defect that can be closed after the QA retesting or can be closed if the defect is duplicate or considered as NOT a defect.
* Reopened - When the defect is NOT fixed, QA reopens/reactivates the defect.
* Deferred - When a defect cannot be addressed in that particular cycle it is deferred to future release.
* Rejected - A defect can be rejected for any of the 3 reasons; viz - duplicate defect, NOT a Defect, Non Reproducible.

31) Explain the difference between Functional testing and NonFunctional testing

| Functional Testing | Non-functional Testing |
| --- | --- |
| It verifies the operations and actions of an application. | It verifies the behavior of an application. |
| It is based on requirements of customer. | It is based on expectations of customer. |
| It helps to enhance the behavior of the application. | It helps to improve the performance of the application. |
| Functional testing is easy to execute manually. | It is hard to execute non-functional testing manually. |
| It tests what the product does. | It describes how the product does. |
| Functional testing is based on the business requirement. | Non-functional testing is based on the performance requirement. |

**Examples:**

**1.** Unit Testing **Examples:**

**2.** Smoke Testing **1.** Performance Testing

**3.** Integration Testing

**4.** Regression Testing

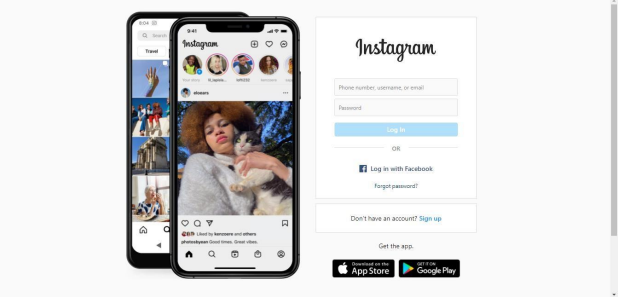
**2.** Load Testing

**3.** Stress Testing

**4.** Scalability Testing

• **To create HLR & TestCase of**

**1)(Instagram , Facebook) only first page**



2) Facebook Login Page : <https://www.facebook.com/>



32) What is the difference between the STLC (Software Testing Life Cycle) and SDLC (Software Development Life Cycle)?

| SDLC | STLC |
| --- | --- |
| SDLC is mainly related to software development. | STLC is mainly related to software testing. |
| Besides development other phases like testing is also included. | It focuses only on testing the software. |
| SDLC involves total six phases or steps. | STLC involves only five phases or steps. |
| In SDLC, more number of members (developers) are required for the whole process. | In STLC, less number of members (testers) are needed. |
| In SDLC, development team makes the plans and designs based on the requirements. | In STLC, testing team(Test Lead or Test Architect) makes the plans and designs. |
| Goal of SDLC is to complete successful development of software. | Goal of STLC is to complete successful testing of software. |
| It helps in developing good quality software. | It helps in making the software defects free. |
| SDLC phases are completed before the STLC phases. | STLC phases are performed after SDLC phases. |
| Post deployment support , enhancement , and update are to be included if necessary. | Regression tests are run by QA team to check deployed maintenance code and maintains test cases and automated scripts. |
| Creation of reusable software systems is the end result of SDLC. | A tested software system is the end result of STLC. |

33) What is the difference between test scenarios, test cases, and test script?

. **Test Scenarios:**  A Test Scenario is any functionality that can be tested. It is also called Test Condition or Test Possibility.

**Test Cases:**  It is a document that contains the steps that has to be executed, it has been planned earlier.

**Test Script:**It is written in a programming language and it's a short program used to test part of functionality of the software system. In other words, a written set of steps that should be performed manually.

34)Explain what Test Plan is? What is the information that should be covered?

Test planning, the most important activity to ensure that there is initially a list of tasks and milestones in a baseline plan to track the progress of the project. It also defines the size of the test effort.

It is the main document often called as master test plan or a project test plan and usually developed during the early phase of the project.

## Test Planning Activities:

* To determine the scope and the risks that need to be tested and that are NOT to be tested.
* Documenting Test Strategy.
* Making sure that the testing activities have been included.
* Deciding Entry and Exit criteria.
* Evaluating the test estimate.
* Planning when and how to test and deciding how the test results will be evaluated, and defining test exit criterion.
* The Test artefacts delivered as part of test execution.
* Defining the management information, including the metrics required and defect resolution and risk issues.
* Ensuring that the test documentation generates repeatable test assets.

35)What is priority?

Priority is defined as the order in which the defects should be resolved. The priority status is usually set by the testing team while raising the defect against the dev team mentioning the timeframe to fix the defect. The Priority status is set based on end users requirement.

For example: If the company logo is incorrectly placed in the company's web page then the priority is high but it is of low severity.

## Priority List:

Priority can be marked as either of the following states:

* **Low -**This defect can be fixed after the critical ones are fixed.
* **Medium -**The defect should be resolved in the subsequent builds.
* **High -**The defect must be resolved immediately because the defect is affecting the application to a considerable extent and the relevant modules cannot be used until it's fixed.
* **Urgent -**The defect must be resolved immediately because the defect is affecting the application or the product severely and the product cannot be used until it has been fixed.

36)What is severity?

Severity means the seriousness of the defect in the product functionality. The test engineer determines the severity level of the defect. It is driven by functionality.

37) Bug categories are…

1. **Software Bugs by Nature:**  
   Software bugs have different natures where they affect the overall functioning of the software differently. Though there are dozens of such bugs existing currently, you may not face them frequently. With that in mind, here are the most common software bugs categorized by nature that you are most likely to witness at some point in your software development career.
   * **Performance Bugs:**  
     No user wants to use software with poor performance. Software bugs that lead to degraded speed, stability, increased response time, and higher resource consumption are considered performance bugs. The most significant sign of any such bug in software is by noticing slower loading speed than usual or analyzing the response time. If any such sign is found, the developer may begin diagnosing a performance bug. The [performance testing](https://www.thinksys.com/performance-testing-services/) phase is part of the development process where every such bug is detected in the software.
   * **Security Bugs:**  
     While using software, security is the biggest concern of a user. Software with poor security will not only put the user’s data at risk but will also damage the overall image of the organization which may take years to recuperate. Due to their high severity, security bugs are considered among the most sensitive bugs of all types. Though it is self-explanatory, security bugs may make the software vulnerable to potential cyber threats. Sometimes, the software organization may not notice such attacks whereas in some cases, these attacks could cause monetary loss to the users, especially small and medium-scale businesses. XSS vulnerabilities, logical errors, and encryption errors are some of the commonest security bugs found in the software. Developers put special focus on checking the code to find any underlying [security bug](https://www.thinksys.com/security-testing-services/) to minimize the risk of cyber-attacks.
   * **Unit Level Bugs:**  
     Unit level bugs are fairly common in software development and do not cause much damage to it as well. Facing basic logic bugs or calculation errors are considered unit-level bugs. The [testing team](https://www.thinksys.com/software-testing-services/) along with the agile team test a small part of the code as a whole. The reason why this testing method is preferred is to make sure that the entire code is working as it is meant to. While testing, the team may encounter unit-level bugs which can be fixed easily as the team is only working with a small code.
   * **Functional Bugs:**  
     Software is as good as the feature it provides. If any of the functionality of a software is compromised, the number ofusers will start to decline drastically until it becomes functional again. A functional bug is when a certain feature or the entire software is not functioning properly due to an error. The severity of such bugs depends on the feature they are hampering. For instance, an unresponsive clickable button that is not functioning is not as severe as the entire software not working. [Functional testing](https://www.thinksys.com/functional-testing-services/) is done by the testing team to identify any such software bug causing functionality errors. Once identified, the team decides its further classification and severity.
   * **Usability Bugs:**  
     Probably one of the most catastrophic bugs for software, a usability bug or defect can stop the software from working to its potential or make it entirely unusable. Examples of this bug in software testing are the inability to log in to the user account or the inefficient layout of the software for the user. The bottom line is that this type of defect or bug can make it complex for the user to use the software efficiently. The developers and engineers have to look out for the right [usability requirements](https://www.thinksys.com/qa-testing/complete-guide-to-usability-testing/) while testing the code to identify such bugs.
   * **Syntax Errors:**  
     Syntax errors are among the commonest software bug types and do not allow the application to be compiled appropriately. This bug occurs due to an incorrect or missing character from the source code due to which the compiling will be affected. A small error like a missing bracket could lead to this problem. The development or testing team will get to know about this bug during compiling and will further analyze the source code to fix the missing or wrong characters.
   * **Compatibility Errors:**  
     Whenever a software or an application is not compatible with hardware, or an operating system, it is considered as incompatible software or a compatibility error. Finding a compatibility error is not a common practice as they may not show up in the initial testing. Due to this reason, the developers should go for compatibility testing to make sure that their created software is compatible with common hardware and operating systems.
   * **Logic Bugs:**  
     Another one of the most frequently found bugs in a software code, logic errors make the software give wrong output, software crash or failure. In the majority of cases, these bugs are caused due to coding errors where it may make the software stuck in a never-ending loading loop. In that case, only an external interruption or software crashing are the two only things that can break the loading loop.
2. **Priority-Based Software Bugs:**  
   The foremost category here is priority-based software bugs. These are based on the impact these bugs leave on the business. Here, the developers will analyze the bug to determine its impact and its defect priority. Afterward, the timeline is given to each bug where it should be rectified within the stipulated time frame to minimize the bug effect on the user. Here are the four types of priority-based software bugs.
   * **Low-priority defects:**  
     Low priority defects do not cause much impact on the functioning of the application. Rather, they are more about software aesthetics. For instance, any issue with the spelling or the alignment of a button or text could be a low-priority defect. The software testing will move to the exit criteria even if the low-priority defects are not fixed, but they should be rectified before the final release of the software.
   * **Medium-priority defects:**  
     Akin to low-priority defects, medium-priority defects do not cause any significant impact on the software, but they should be fixed in any subsequent or upcoming release. Such defects may not have the same effect for every user and it may vary with the device as well as specific configuration they have.
   * **High-priority defects:**  
     Unlike the previous two, the exit criteria of high-priority defects are not met until the issue is resolved. Every bug falling in this category may make certain features of the software unusable. Even though it may not affect every user, it is mandatory to fix these bugs before any further step is taken in software development or testing.
   * **Urgent Defects:**  
     As the name suggests, all bugs that should be dealt with utmost urgency fall under this category. Urgent defects may leave a lasting impact on the brand image as well as affect the userexperience drastically. The stipulated timeline for fixing these bugs is within 24-hours of reporting.
3. **Software Bugs by Severity:**  
   Depending on the technical effect that the bug will cause on the software, the bugs are categorized into four categories.
   * **Low Severity Bugs:**  
     Low severity bugs do not cause much damage to the functioning of the software as their primary target is the user interface. For instance, the font of the text on the program differs from what was used. These bugs can be fixed easily and are nothing to worry about.
   * **Medium Severity Bugs:**  
     Every bug that can affect the functionality of the software a little bit is considered a medium severity bug. All such bugs make the software function different from what it is supposed to function. Though they are not also major for the program, they should be fixed for a better user experience.
   * **High Severity Bugs:**  
     High severity bugs affect the software functionality, making it behave differently from what it was programmed for. Not only are such bugs damaging for the software, they sometimes make the entire software unusable for the user.
   * **Critical Bugs:**  
     Critical bugs are the most damaging bugs in the category that can hinder the functionality of the entire software. The reason why critical bugs are considered the most damaging is that further testing on the software becomes impossible till such bugs exist in the software.

38)Advantage of Bugzila .

**The Advantages of Bugzilla are:**

* it is an open-source widely used bug tracker;
* it is easy in usage and its user interface is understandable for people without technical knowledge;
* it easily integrates withtest management instruments;
* it integrates with an e-mailing system;
* it automates documentation.

Not all testers like to work with [Bugzilla](https://qatestlab.com/approach/technologies/bug-tracking-tools/). Some of them find that its interface is too sophisticated, complain that it is hard to manage the logged in errors and that there are many defects in the code of this instrument.

39) What are the different Methodologies in Agile Development Model?

Agile refers to the methods and best practices for organizing projects based on the values and principles documented in the [Agile Manifesto](https://www.agilealliance.org/agile101/what-is-agile/). However, there’s no one right way to implement Agile and many different types of methodologies from which to choose. Here are some of the most common Agile frameworks.

#### Kanban

Kanban is a simple, visual means of managing projects that enables teams to see the progress so far and what’s coming up next. Kanban projects are primarily managed through a Kanban board, which segments tasks into three columns: “To Do,” “Doing,” and “Done.”

#### Scrum

Scrum is similar to Kanban in many ways. Scrum typically uses a Scrum board, similar to a Kanban board, and groups tasks into columns based on progress. Unlike Kanban, Scrum focuses on breaking a project down into sprints and only planning and managing one sprint at a time. Scrum also has unique project roles: Scrum master and product owner.

#### Extreme Programming (XP)

Extreme Programming (XP) was designed for Agile software development projects. It focuses on continuous development and customer delivery and uses intervals or sprints, similar to a Scrum methodology. However, XP also has 12 supporting processes specific to the world of software development:

* Planning game
* Small releases
* Customer acceptance tests
* Simple design
* Pair programming
* Test-driven development
* Refactoring
* Continuous integration
* Collective code ownership
* Coding standards
* Metaphor
* Sustainable pace

#### Feature-driven development (FDD)

Feature-driven development is another software-specific Agile framework. This methodology involves creating software models every two weeks and requires a development and design plan for every model feature. It has more rigorous documentation requirements than XP, so it’s better for teams with advanced design and planning abilities. FDD breaks projects down into five basic activities:

* Develop an overall model
* Build a feature list
* Plan by feature
* Design by feature
* Build by feature

#### Dynamic Systems Development Method (DSDM)

The Dynamic Systems Development Method (DSDM) was born of the need for a common industry framework for rapid software delivery. Rework is to be expected, and any development changes that occur must be reversible. Like Scrum, XP, and FDD, DSDM uses sprints. This framework is based on eight fundamental principles:

* Focus on the business need
* Deliver on time
* Collaborate
* Never compromise quality
* Build incrementally from firm foundations
* Develop iteratively
* Communicate continuously and clearly
* Demonstrate control

#### Crystal

Crystal is a family of Agile methodologies that includes Crystal Clear, Crystal Yellow, Crystal Orange, Crystal Red, etc. Each has a unique framework. Your choice depends on several project factors, such as your team size, priorities, and project criticality.

#### Lean

Lean development is often grouped with Agile, but it’s an entirely different methodology that happens to share many of the same values. The [main principles of the Lean methodology](https://leankit.com/learn/lean/principles-of-lean-development/) include:

* Eliminating waste
* Build quality in
* Create knowledge
* Defer commitment
* Deliver fast
* Respect people
* Optimize the whole

40)Explain the difference between Authorization and Authentication in Web testing.

| Authentication | Authorization |
| --- | --- |
| In the authentication process, the identity of users are checked for providing the access to the system. | While in authorization process, a the person’s or user’s authorities are checked for accessing the resources. |
| In the authentication process, users or persons are verified. | While in this process, users or persons are validated. |
| It is done before the authorization process. | While this process is done after the authentication process. |
| It needs usually the user’s login details. | While it needs the user’s privilege or security levels. |
| Authentication determines whether the person is user or not. | While it determines What permission does the user have? |
| Generally, transmit information through an ID Token. | Generally, transmit information through an Access Token. |
| The OpenID Connect (OIDC) protocol is an authentication protocol that is generally in charge of user authentication process. | The OAuth 2.0 protocol governs the overall system of user authorization process. |
| Popular Authentication Techniques-   * Password-Based Authentication * Passwordless Authentication * 2FA/MFA (Two-Factor Authentication / Multi-Factor Authentication) * Single sign-on (SSO) * Social authentication | Popular  Authorization Techniques-   * Role-Based Access Controls (RBAC) * SON web token (JWT) Authorization * SAML Authorization * OpenID Authorization * OAuth 2.0 Authorization |
| The authentication credentials can be changed in part as and when required by the user. | The authorization permissions cannot be changed by user as these are granted by the owner of the system and only he/she has the access to change it. |
| The user authentication is visible at user end. | The user authorization is not visible at the user end. |
| The user authentication is identified with username, password, face recognition, retina scan, fingerprints, etc. | The user authorization is carried out through the access rights to resources by using roles that have been pre-defined. |
| **Example**: Employees in a company are required to authenticate through the network before accessing their company email. | **Example:** After an employee successfully authenticates, the system determines what information the employees are allowed to access. |

**What are the common problems faced in Web testing?**

# 5 Web Application Testing Challenges

Testing is a fundamental challenge when developing web applications. Different browsers, interfaces, security threats, and overall app integration are just a few of the issues faced by developers. Since testing is a crucial phase in the development process, the developer should expect to run into unforeseen issues associated with both the web application, and the testing process itself. Each primary issue associated with testing has the potential to branch into uncountable related issues, all of which can be solved if properly

identified. Below are five web application testing challenges faced by web developers during the development process.

## Integration

Integration testing exposes problems with interfaces among different program components before deployment. Additionally, integration testing can show the different issues an application may have when interacting with other applications, allowing the developer to tweak things. Environment and infrastructure inconsistency, different interaction models, and overall performance are just a few of the issues associated with integration testing.

## Interoperability

Proving end-to-end functionality between communicating systems is always a challenging obstacle. Different users utilize different browsers and operating systems. To pull data, testing each one to confirm a clear information pathway is very important. Even if the browsers are similar, the web application may be rendered differently based on screen resolution and overall software configuration. This can present some serious issues for developers.

## Security

In one of the most important tests, the developer must make sure that the continually evolving cyber threat can be countered and neutralized. Additionally, tests associated with data integrity before and after an attack are equally important when considering data breaches or lost information. Some of the challenges associated with security testing include dealing with unsecured communications, removing malicious files (if security firewalls have been breached), and the utilization (and integration) of different authentication procedures.

## Performance

Slow applications are not successful. Developers understand that the speed of the app is defined by the need of the user, and with more users expecting more speed, the requirement of performance is non-negotiable. Testing large applications on minimal hardware, underestimating software requirements, and overextending application features are just a few of the issues associated with performance testing. Integration and interoperability issues can also have a direct effect on performance, and because of that, should be tested at the beginning.

## Usability

Since web-based applications are dependent on different browsers, consistent usability is crucial. Additionally, since the app is the brand (or a component thereof), any inconsistency within the user experience may translate into a negative experience, affecting the brand and its potential growth. When testing usability, developers face issues with scalability and interactivity. Since every user is different, it is important for developers to utilize a representative group to test the application across different browsers, using different hardware.

The testing process is inherently full of issues, but each issue faced by the developer is one less that will be faced by the user. In app development, the first interaction with the app needs to be as flawless as possible, allowing the user to adopt and use the app in a way that is as effortless as possible. Bytesting integration, interoperability, security, performance, and usability, developers will be better able to identify and manage the actual issues associated with the app. In the end, it is about a positive user experience.

**To create HLR & TestCase of WebBased (WhatsApp web , Instagram) 1. WhatsAppWeb :** [**https://web.whatsapp.com**](https://web.whatsapp.com)

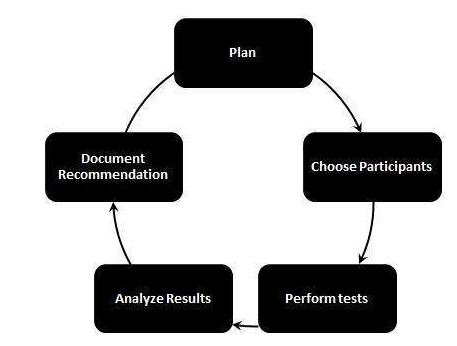


• When to used Usablity Testing?

Usability testing, a non-functional testing technique that is a measure of how easily the system can be used by end users. It is difficult to evaluate and measure but can be evaluated based on the below parameters:

* Level of Skill required to learn/use the software. It should maintain the balance for both novice and expert user.
* Time required to get used to in using the software.
* The measure of increase in user productivity if any.
* Assessment of a user's attitude towards using the software.

## Usability Testing Process:



• **What is the procedure for GUI Testing?**

**Graphical User Interface Testing (GUI) Testing** is the process for ensuring proper functionality of the graphical user interface (GUI) for a specific application.GUI testing generally evaluates a design of elements such as layout, colors and also fonts, font sizes, labels, text boxes, text formatting, captions, buttons, lists, icons, links, and content. GUI testing processes may be either manual or automatic and are often performed by third-party companies, rather than developers or end users.

**Feature of Graphical User Interface Testing (GUI):**   
There are some feature of GUI which are given below:

* It provides a customizable test report.
* It is run tests in parallel or distributed on a Selenium Grid with built-in Selenium Webdriver.
* It allows you to test the functionality from a user’s perspective.
* Sometimes the internal functions of the system work correctly but the user interface doesn’t then GUI testing is good to have in addition to the other types.
* It provides reliable object identification, even for web elements with dynamic IDs.