**Adhoc Testing**

The meaning of word ***Ad-Hoc*** is something which is not in order or not organised or unstructured. Similarly when a ***software testing*** is performed without following any formal process like requirement documents, test plan , ***test cases***, etc. it is said to be Adhoc Testing. While executing the ad-hoc testing there is NO formal process of testing which can be documented. Ad hoc Testing is also known as ***Random Testing*** or ***Monkey Testing***



Adhoc Tests are done after formal testing is performed on the application. Testing is carried out with the knowledge of the ***tester*** and the tester tests randomly without following the specifications/requirements. Hence the success of Adhoc testing depends upon the capability of the tester, who carries out the test. ***Defects*** found using this method are hard to reproduce as there are no written test cases. Sometimes it can find holes or defects in the test strategy and can expose relationships between subsystems which would never have been found if written test cases existed.

The advantage of Ad-hoc testing is to check for the completeness of testing and find more defects than planned testing. The defect catching test cases are added as additional test cases to the planned test cases. Ad-hoc Testing saves lot of time as it doesn’t require elaborate test planning , documentation and test case design.

### *****When to execute Adhoc Testing?*****

Ad-hoc testing can be done at any point of time whether it’s beginning, middle or end of the project testing. Ad hoc testing can be performed when the time is very limited and detailed testing is required. Usually adhoc testing is performed after the formal test execution. Ad hoc testing will be effective only if the tester is having thorough knowledge of the System Under Test.

This testing can also be done when the time is very limited and detailed testing is required.

### Forms of Adhoc Testing :

***Buddy Testing:***Two buddies, one from development team and one from test team sit together and work on that particular module to avoid from building the invalid ***test scenarios*** and help the tester from reporting the invalid defects. This kind of testing happens usually after completing the ***unit testing***.

***Pair Testing***:Two testers are assigned the same modules and they share ideas and work on the same systems to find defects. One tester executes the tests while another tester records the notes on their findings. The aim of this type of testing is to come up with maximum testing scenarios so that the entire module should have complete test coverage.

***Monkey Testing***:Testing is performed randomly, with some random data, without any test cases with the aim of breaking the system.

### *****Difference between Buddy and Pair Testing*****

***Buddy Testing*** is combination of ***Unit Testing*** and ***System Testing*** together with developers and testers but ***Pair Testing*** is done only with the testers with different knowledge levels. Experienced and non-experienced share their ideas and views with the tester.

# What is an Incident And Incident Report in software testing?

## What is an Incident?

While testing if the actual result varies from expected result it is referred to as ***bug, defect, error, problem, fault or an incident***. Most often, all of these terms are synonymous. But Incidents can be defined in simple words as an event encountered during testing that requires review.

Every incident that occurs during testing may not be a defect or bug. An incident is any situation in which the software system has a questionable behavior, however we call the incident a defect or bug only if the Root Cause is the problem in the tested component and not other factors like test environment/test scripting issues.

***ISTQB Definition*** : Any event occurring that requires investigation.

Other causes of incidents include mis-configuration or failure of the test environment, corrupted test data, bad tests, invalid expected results and tester mistakes.

## What is Incident Report?

After logging the incidents that occur in the field or after deployment of the system we also need some way of reporting, tracking, and managing them. In some projects, a very large number of defects are found. Even on smaller projects where 100 or fewer defects are found, it is very difficult to keep track of all of them unless we have a process for reporting, classifying, assigning and managing the defects.

Incidence report is the detailing for any test that failed, when it failed and any supporting evidence intended to throw light on why a test has failed. This document is deliberately named as an ***Incident Report***, and not a fault report, as discrepancy between expected and actual results can occur for a number of reasons other than a fault in the system. The most common defects reported are against the code or the system itself. However, in some cases, defects are reported against requirements and design specifications, user and operator guides and tests also.

Incidence report helps to have clear goals in mind when writing. One common goal for such reports is to provide programmers, managers and others with detailed information about the behavior observed and the defect.

### *****What is the Difference between Incident and Defect?*****

Not all the Incident are defect, but all the defects are incidents. In other words unpleasant incidents are defects. Some of the incidents are because of failure in configuration issues these cannot be a bug.

* Incident= Any event occurring that requires investigation.
* Defect= Any flaw in a component/system that can cause a component/system to fail to perform its required functionality.

## What is Incident Management?

Incident management is the overall process starting from logging incidents to resolving them.

It is a very critical process as this will ensure that the incidents get addressed is a systematic and effective manner. Also, by streamlining the entire process, there is a good chance that early fixing of the issues might happen.