L10: Inclass activity

1. Smoke Test: Also known as sanity testing, it is a quick and basic test to check if the major functionalities of the software work correctly. Smoke tests are usually performed after a build to ensure stability before further testing.

2. Regression Test: This type of testing ensures that new changes or modifications in the software do not adversely affect the existing functionalities. It involves retesting the unchanged parts of the software along with the newly added features.

3. Integration Test: Integration testing focuses on testing the interaction between different modules or components of the software. It verifies that the integrated components work together as expected and identifies any interface issues or integration bugs.

4. Unit Test: Unit testing involves testing individual units or components of the software in isolation. Developers typically perform unit tests to ensure that each unit functions correctly as per design specifications.

5. Functional Test: Functional testing verifies that the software functions according to the specified requirements. It involves testing various functionalities of the software by providing input and checking if the output matches the expected behavior.

6. Performance Test: Performance testing evaluates the responsiveness, scalability, and stability of the software under various workload conditions. It helps identify performance bottlenecks, such as slow response times or resource constraints.

7. Acceptance Test: Acceptance testing, also known as user acceptance testing (UAT), is performed to validate if the software meets the end-user requirements and business needs. It is usually conducted by the end-users or stakeholders to ensure that the software is ready for production release.

8. Security Test: Security testing aims to identify vulnerabilities and weaknesses in the software that could be exploited by attackers. It involves testing for authentication, authorization, encryption, and other security mechanisms to ensure the confidentiality, integrity, and availability of data.