**Security Test Evaluation and Reporting:**

Measuring the test results and evaluating the status with respect to security expectations and exit criteria or acceptance criteria are required to determine the test completion.

**Security Test Evaluation** is needed because rise of new threats, lead to higher level security, than the initial level of security testing.

**Security Test Reporting:**

**Confidentiality of Security Test Results:**

By evaluating the security implementation, one may find the hidden holes and vulnerabilities,

Lies may lead to communicate the mislead information.

One should be conservative while sharing the test reports to stakeholders, it should not be shared with the all the people.

**Creating Proper Controls and Data Gathering Mechanism for Reporting Security Test Status:**

Security defects have more impact and are categorized as higher severity compared to the functional defects.

Higher focus on security defects, their risks and their possibles resolution.

**Analysing Interim Security Test Status Reports:**

1.Report Identifier

2.Summary

Executive Summary

**The effectiveness of security testing reporting depends on the following:**

• The timing of the report.

• The content of the report.

• The recipients of the report.

• The tuning of the content to match the recipients’ need for the information Multiple reports may be required to meet the needs of various stakeholders. For example, the content of a report for executive management will not be the same as the content for a system architect.