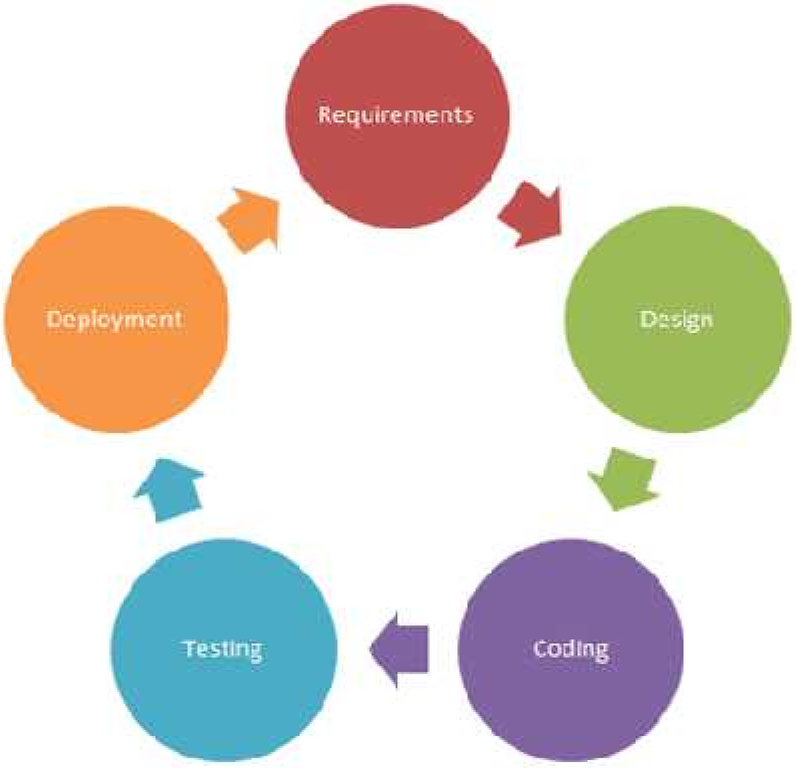
Module 3 Secure Software Development Life Cycle (SDLC)

Software Development Life Cycle (or SDLC) is the process which is followed to develop a software product. It is a structured way of building software applications. Most organizations have a process in place for developing software; this process may, at times, be customized based on the organizations requirement and framework followed by organization.

Classical SDLC Model –



Sample SDLC Process

- Requirements Gathering

  A Software Requirement Specification or SRS is a document which records expected behavior of the system or software which needs to be developed.

- Design

Software design is the blueprint of the system, which once completed can be provided to developers for code development. Based on the components in design, they are translated into software modules/functions/libraries, etc… and these pieces together form a software system.

- Coding

  During this phase, the blueprint of the software is turned to reality by developing the source code of the entire application. Time taken to complete the development depends on the size of the application and number of programmers involved.

- Testing

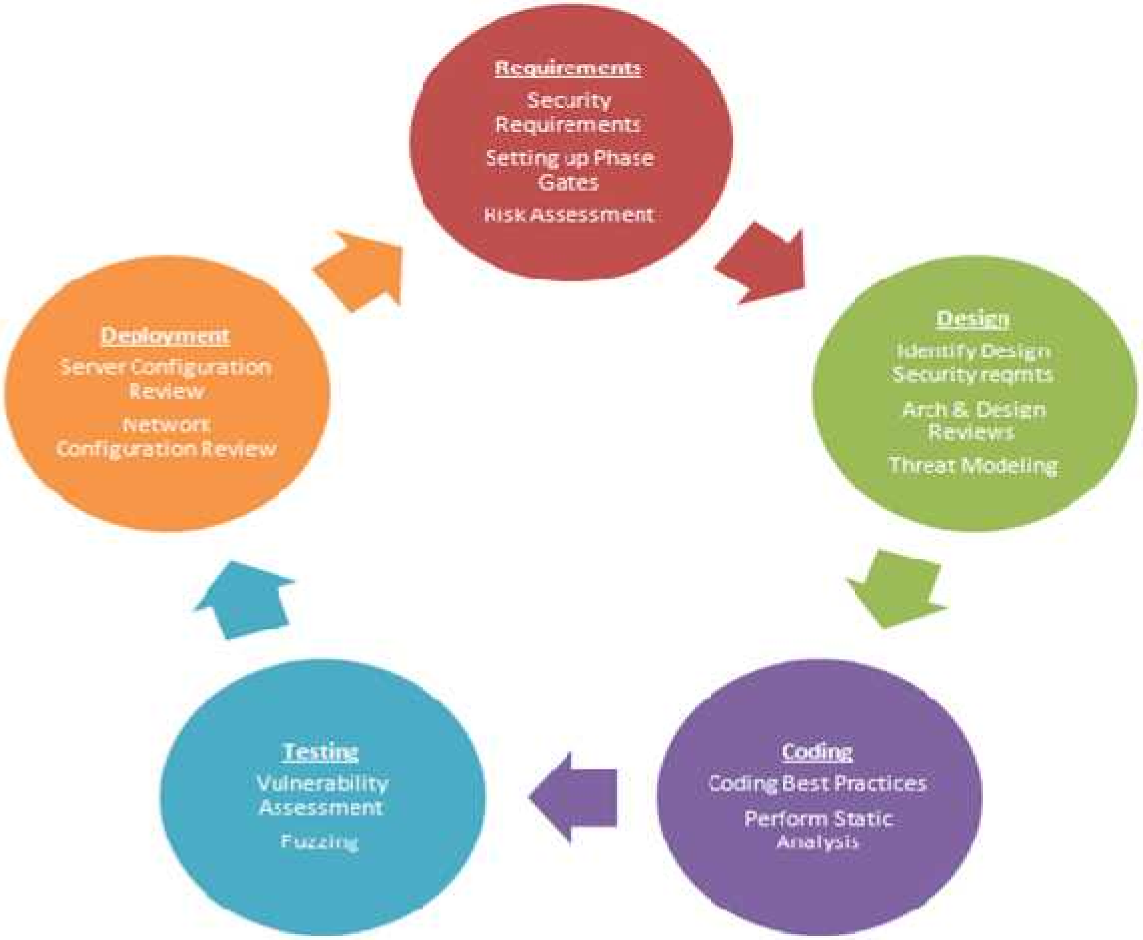
  Once the application development is completed, it is tested for various issues like functionality, performance, and so on. This is to ensure that the application is performing as expected. If there are any issues, these issues are fixed before/after going to production depending on the nature of issue and the urgency to go live for the application.

- Deployment

  Once the application is ready to go live, it is deployed on a production server in this phase. If it is developed for a client, the deployment happens in a client premise or datacenter where there client wants to get the application installed.

Secure SDLC –

S-SDLC stresses on incorporating security into the Software Development Life Cycle. Every phase of SDLC will stress security – over and above the existing set of activities. Incorporating S-SDLC into an organization’s framework has many benefits to ensure a secure product.



Sample S-SDLC

Each phase of the Sample SDLC is mapped with security activities, as demonstrated in the figure and as explained below:

- Requirements Gathering
    - Security Requirements
    - Setting up Phase Gates
    - Risk Assessment
- Design
    - Identify Design Requirements from security perspective
    - Architecture & Design Reviews

    - Threat Modeling
- Coding
    - Coding Best Practices
    - Perform Static Analysis
- Testing
    - Vulnerability Assessment
    - Fuzzing
- Deployment
    - Server Configuration Review
    - Network Configuration Review