Q:1:- Introduction to software quality assurance:

- Learning about the software development life cycle (SDLC) and its phases?

Ans:- Introduction to software quality assurance:

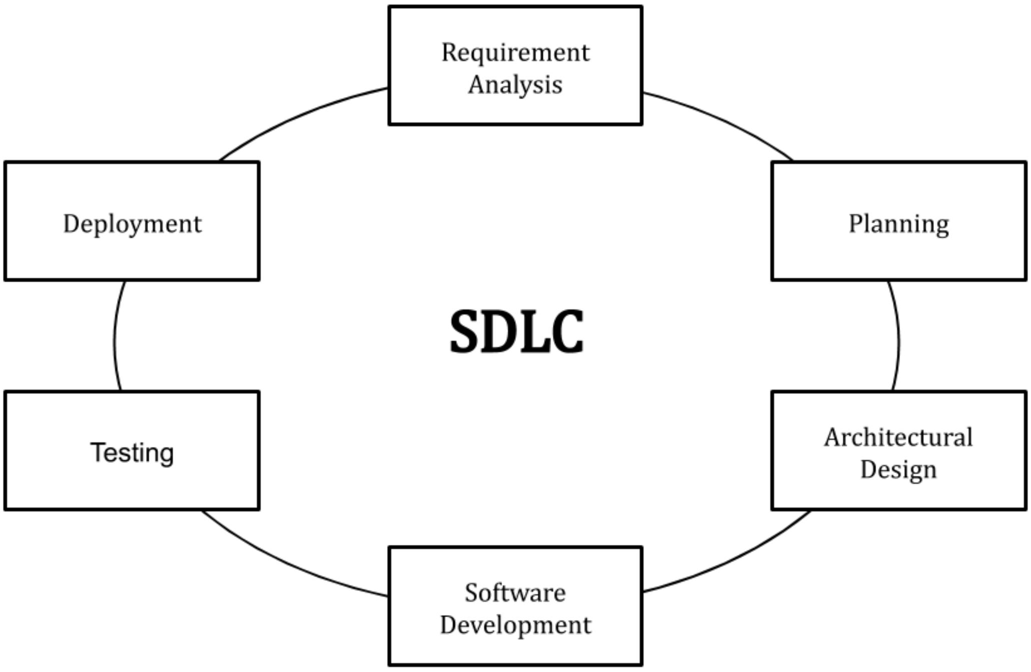
Software Quality Assurance (SQA) is a set of systematic activities and processes carried out to ensure that software products and services meet defined quality standards. It encompasses a range of activities aimed at preventing defects, detecting and resolving issues, and ensuring that software meets the specified requirements and user expectations.

The primary goal of Software Quality Assurance is to establish and maintain high-quality software throughout the software development life cycle (SDLC). It involves a combination of techniques, methodologies, and tools to assess and improve the quality of software products, processes, and resources. SQA is typically implemented by a dedicated team or department within an organisation, responsible for overseeing the quality of software projects.

Software Development Life Cycle:

SDLC or the Software Development Life Cycle is a process that produces software with the highest quality and lowest cost in the shortest time possible. SDLC provides a well-structured flow of phases that help an organisation to quickly produce high-quality software which is well-tested and ready for production use.

The SDLC involves six phases as explained in the introduction. Popular SDLC models include the Waterfall , Spiral Model & Agile Model.



1: Planning and Requirement Analysis: Here, security requirements and appropriate security choices that can mitigate potential threats and vulnerabilities are identified in this stage. What security design principles and best practices to be used are also thought about here.

2: Architectural Design: The development team uses the security design principle and architecture to consider potential risks. This stage involves threat modelling, access control, encryption mechanism, and architecture risk analysis.

3: Software Development and Testing: The code reviews are done to ensure software follows code standards and security controls are implemented. Security vulnerability tests like penetration testing are also done to identify potential issues.

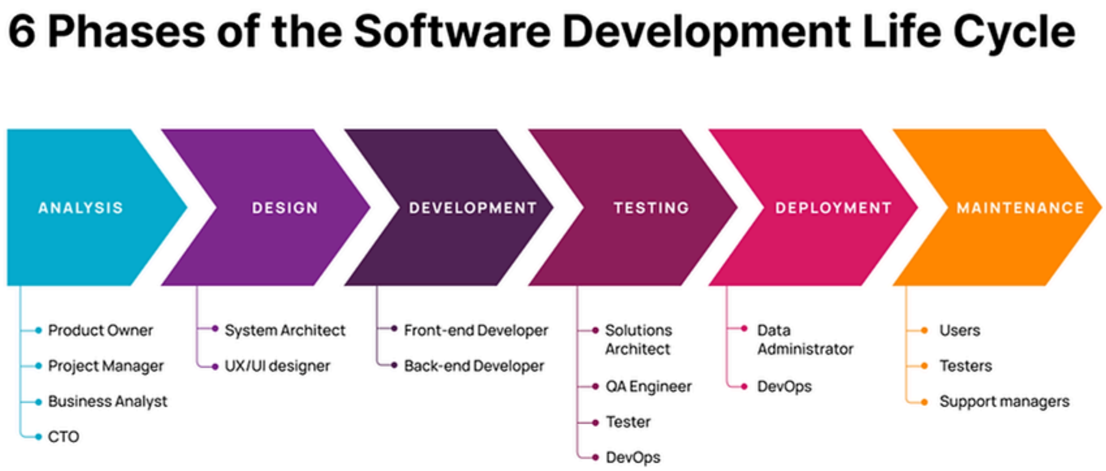
4: Deployment: Automated DevSecOps tools are used to improve application security. To ensure the software is deployed securely, firewalls, access controls, and security settings are configured.

5: Maintenance: Security continues after deployment. The team must continuously monitor the software for security vulnerabilities. The team would also update the software with security patches and updates as necessary.

Benefits of the SDLC:

SDLC done right can allow the highest level of management control and documentation. Developers understand what they should build and why. All parties agree on the goal upfront and see a clear plan for arriving at that goal. Everyone understands the costs and resources required.

Several pitfalls can turn an SDLC implementation into more of a roadblock to development than a tool that helps us. Failure to take into account the needs of customers and all users and stakeholders can result in a poor understanding of the system requirements at the outset. The benefits of SDLC only exist if the plan is followed faithfully.


6 Phases of the Software Development Life Cycle
ANALYSIS
Product Owner
Project Manager
Business Analyst
CTO
DESIGN
System Architect
UX/UI designer
DEVELOPMENT
Front-end Developer
Back-end Developer
TESTING
Solutions Architect
QA Engineer
Tester
DevOps
DEPLOYMENT
Data Administrator
DevOps
MAINTENANCE
Users
Testers
Support managers