Software Development Lifecycle (SDLC)

The current security standards advise to implement Security by Design. The purpose is to incorporate security from the start. Security needs to be implemented in each level of your software development, because security is more than only policies or documents.

Security needs to be implemented at:

- Governance level
- Definition and design phases
- Development phases
- Deployment phases
- Maintenance and operations

There are several frameworks like OpenSAMM or BSIMM to support your SDLC lifecycle and evolution.

Your application building, testing and deployment process must implement:

- Verification that none of your components and third-party libraries have no vulnerabilities or security issues.
- Tests that ensure that the application shows no known vulnerabilities to any type of malicious code.
- Dependency management so third-party libraries can be checked for security issues in vulnerability databases.
- When deploying applications or mobile apps all debugging information and settings must be disabled
- A mobile app need to be signed and obfuscated.