**ARBA MINCH UNIVERSITY INSTITU OF TECHNOLOGY**



***FACULITY OF COMPUTING AND SOFTWARE ENGINEERING***

***DEPARTMENT OF SOFT WARE ENGINEERING***

***SUBMISSION DATE: 10/02/2020 G.C***

***SUBMITTED TO: M.R YOHHANNIS***

1. ***Explain the security measures taken on each (7) phases of SDLC(software development life cycle)***
2. *Planning phase*
3. *Requirement analysis phase*

## Incorporate an industry-standard security model

## Assess the landscape

## Educate personnel on software security

Ensure that all personnel involved in the project are knowledgeable and up-to-date with software security standards to reduce insecure design and development practices. [Investing in training your staff](https://www.synopsys.com/software-integrity/training.html) is scalable, and aligns with the overall organization and the scope of each software development project at hand.

* **Assign responsibility of software security**

To ensure that software security is incorporated into the SDLC, creating a [software security group (SSG)](https://www.synopsys.com/blogs/software-security/software-security-group-ssg/) is an effective way to educate, assess, and enforce established security measures across the organization

* **Establish and institute a comprehensive risk management process**

It is critical to your SDLC’s success to identify major risks and execute a mitigation plan. These are also key aspects to:

* Ensure proper security design
* Ensure an effective guide in SDLC execution in terms of:
  + Controlling scope-creep
  + Staying within budget and schedule goals
  + Engaging with stakeholders
* **Perform security-focused requirements gathering**

Tailor your organization’s approach to generating security requirements as a part of the initial phase. This approach will aid in embedding a solid security mindset throughout the SDLC.

1. *Software development stage*
2. *Design and prototyping stage*

* **Perform architecture reviews and threat modeling**

It is far more cost-effective to identify and remediate design flaws early in the design process than to patch flawed design implementations once the software is deployed.

* Analyzing fundamental design principles
* Assessing the attack surface
* Enumerating various threat agents
* Identifying weaknesses and gaps in security controls

1. *Software testing stage*

## **Execute test plans and perform penetration tests**

Execute the test plans during the verification phase.

1. *Implementation and integration stage*

* **Carry out code reviews during implementation**

Along with secure coding standards and static code analyses, perform a [secure code review](https://www.synopsys.com/glossary/what-is-code-review.html) as a condition to passing a release gate.

1. *Operations and maintenance stage*

## *-* **Deploy software product**

Plans for software maintenance and a change management process should be in place at this stage to efficiently handle any bugs or enhancement requests that come out of production. Rollback plans and disaster recovery requirements in this phase also help ensure continued customer confidence.