Article

Oct 2022

Five key parts of the (secure) cycle of life

Secure SDLC is defined as the process of integrating security throughout the software development lifecycle, helping you catch issues in requirements before they manifest as security problems in production.

Shashank Patwardhan
Information Security Consultant

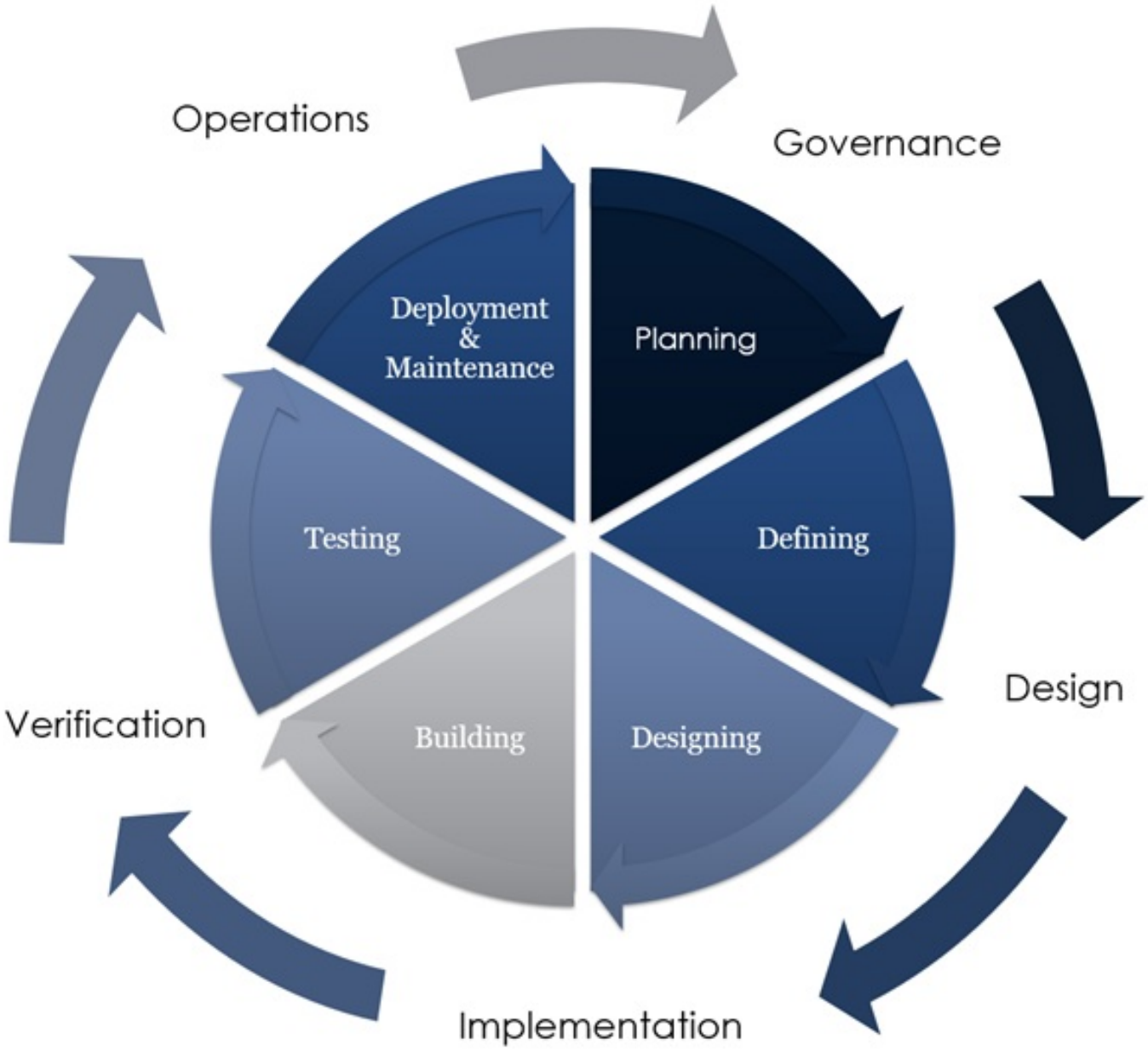
Email shashank.patwardhan@waterstons.com

The software development lifecycle

Many companies only consider security in their application as part of the quality assurance process after their software has been fully developed, towards the end of the SDLC.

Whatever methodology used by the software development organisation, it can always be broken down into different phases – planning, defining, designing, building, testing, and deployment and maintenance.

Historically, AppSec was only considered as part of the testing phase, resulting in high numbers of undetected vulnerabilities, improper handling of private customer data, increased number of data breaches and more expensive SDLC.



1. **Think Security from the start**

Security design principles and methodologies should be embedded within the development teams from the very start ensuring security by design, and that it is tested from day one.

2. **Staff education**

Equip your developers with the latest secure development frameworks and best practice strategies to ensure they are constantly considering security. They will become your human firewall!

3. **Key benefits**

By considering security from the start you can reduce costs, build a more reliable, secure and stable product, align with legal compliance throughout, implement software and updates faster and inspire brand confidence with your marketplace.

4. **Test your controls**

Embedding a robust and automated testing regime to try to make your product fail. With ongoing, regular reviews you can understand the user journey, how you would deal with an incident and get to know it intimately before going live.

5. **Continual improvement**

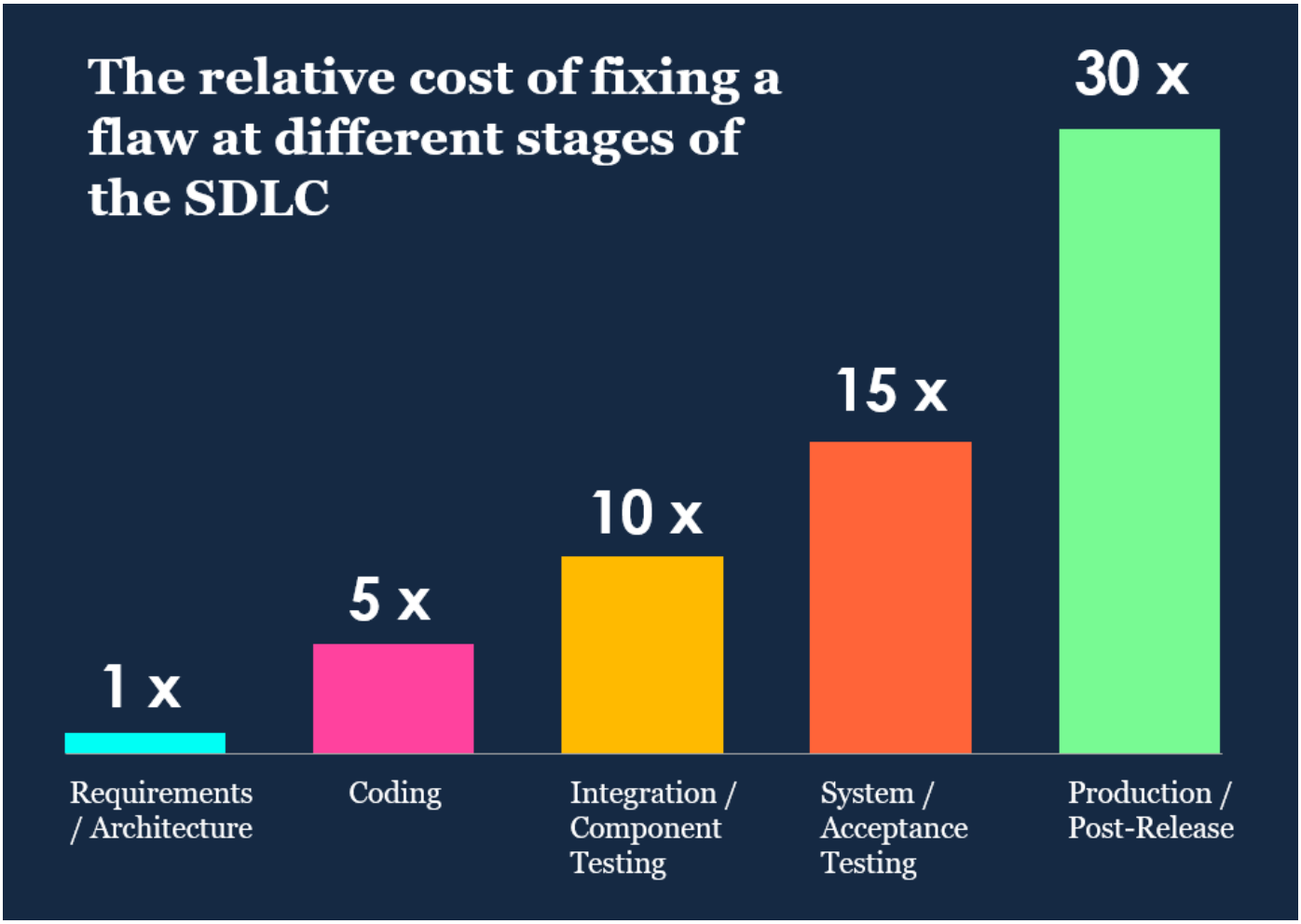
By ensuring you are continually, and consistently, improving your product remains agile and proactive to change in preparation for zero-day situations.

How can secure SDLC provide return on investment?

According to NIST, the cost of removing an application's security vulnerability during the design phase ranges from 30-60 times less than if removed during production.

When AppSec was only a part of the testing phases, it resulted in high numbers of undetected vulnerabilities, improper handling of private customer data, increased data breaches and more expensive SDLC.

But by implementing Secure SDLC, organisations add extra steps to incorporate application security from the start, meaning hackers need to penetrate a variety of application security measures in due to the additional barriers created throughout the process.



If you're developing software, or would like to, and don't know where to start with making it secure, talk to our experts.