General Discussion on Software Development Security for CISSP.

Introduction to Software Development, SDLC, Database and Object Oriented Programming.

Session 1 9/12/2020 Classroom-1

NOTES

Introduction to software development

Does anyone here use a smartphone? I am sure most of us do. The cellphones of today are plagued with Software bugs and flaws in order to sell the flagship product and also outsell it against their competitors product.

Before we go into the SDLC phases and discussion on various phases of software / system development. Let me take you to a very important aspect of SDLC that we need to understand for the CISSP.

And that is Security. Where does security start in your software development?
When do you start thinking about security?
How do you make sure your software is secure?
How do you keep your current software secure from future threats?

Let us talk about the bug in the Elephant's ear.

What are the common flaws?

Bugs in the software (Vulnerabilities) go unnoticed until they are released.

First actual case of bug being found," according to the brainiacs at Harvard, 1945. The engineers who found the moth were the first to literally "debug" a machine.

Nowadays, we see bugs in most applications that are being used in everyday business operations, manufacturing processes and health and information processing systems.

There are two kinds of people who will find these bugs.
Security researchers, bounty hunters or the black hat hackers.
Then the vulnerability is posted on a public site on how it can be exploited.
Then the vendor continues its Software Development Lifecycle type of process to fix the bug or redesign their software.
The patch is then downloaded and installed.

Of Course there are other reasons why the majority of the applications and software released have critical security vulnerabilities. One of the common reasons or too familiar reasons seen is that the software developer does not really understand security or the security professional does not understand software development. This is called Skills gap. That is where we as advisors come into the picture.

SDLC for CISSP.

For the exam, you should be able to describe the models of System Development such as waterfall, spiral model, agile development, also the maturity models such as SW-CMM and IDEAL.

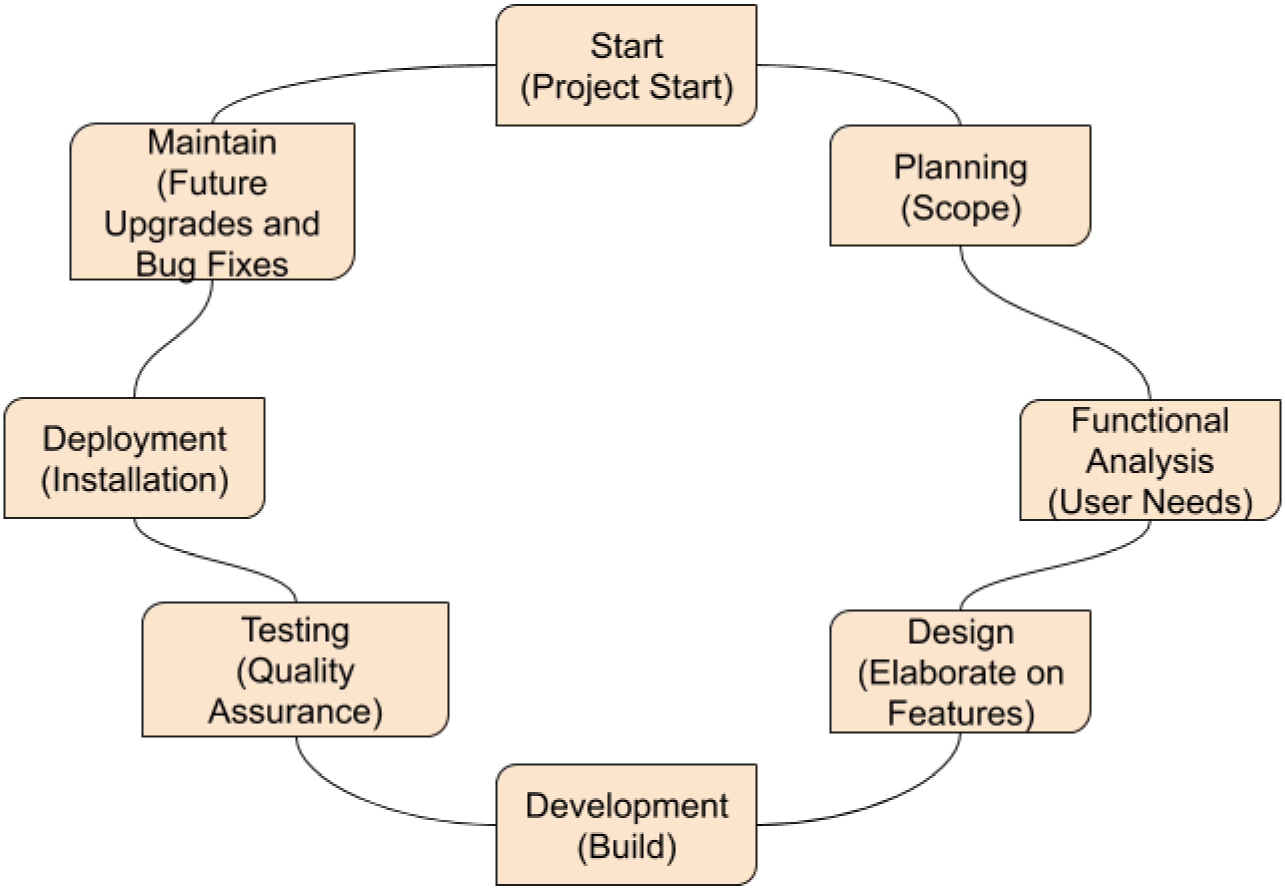
Also know important terms such as DevOps. Which is Development and Operations Combined when developing a software. It is obviously not that simple. You are also combining the Quality Assurance. Again I don't want to go into details on this particular topic. But understanding what Quality Assurance is very important.

SDLC as you may already know stands for Software Development Life Cycle, you can also use it for System Development Life cycle.
SDLC is a set of steps used to create software applications. These steps divide the development process into tasks, which can then be assigned, completed, and measured

What is SDLC?

- It is a framework
- methodology with clearly defined processes for creating high-quality software
- provides a well-structured flow of phases
- There is a strong focus on testing

The different phases in a SDLC



Project Start-
Planning- Feasibility, cost, risk analysis, Management approval, basic security objectives
Functional Analysis - Define need, requirements, review proposed security controls
Design - Develop detailed design specs, Review support documentation, Examine security controls
Software Development - Programmers develop code. Unit testing Check modules. Prototyping, Verification, Validation.

Testing - Separation of duties, security testing, data validation, bounds checking, certification, accreditation, release into production. Certification/accreditation
Deployment : Installation in Production and User Acceptance and Training
Operations and maintenance - Revisions/ Disposal - remove. Sanitation and destruction of unneeded data

References:

NIST SDLC Documentation
https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=902622