Life Cycle Security Integration Help

The standard system- or application-development life cycle (SDLC) comprises five phases, which are discussed at length in the NCI SDLC Roadmap and aligned with the broader Enterprise Performance Life Cycle (EPLC) as defined by the Department of Health and Human Services:

- Initiation and design
- Development or acquisition
- Implementation
- Operations and maintenance
- Retirement or disposal

Regardless of which life cycle model you use, system and information owners must ensure that their federal information systems comply with agency and federal requirements throughout the life of the system. Once a system is deployed and operational, ongoing security requirements such as vulnerability scanning, security patching, configuration management, audit log collection and analysis, and other security-related monitoring and testing must be maintained. If security is overlooked, it often leads to breaches or incidents that require unplanned time and money to remediate, which are usually more costly than integrating proper security measures as part of the system's initial design.

The NCI Information System Security Officer (ISSO) has developed the SDLC Roadmap to help you better understand, plan for, and integrate security into your system by outlining key compliance activities, roles and responsibilities, artifacts, and resources. The more you plan for security at the beginning, and the more you integrate security through automation, the more reliable and cost-effective they will be in the long-run. The concept of DevOps is also gaining interest and traction with many government agencies – including the NIH - but there are currently no requirements to use DevOps. Continuous integration and automated deploy/build/test cycles can be used to address some of the security compliance requirements found in FISMA. As a contractor, you should discuss these concepts and practices with your Contracting Officer Representative (COR) before implementing them to understand how DevOps might address some of the security life cycle needs for your application.

Benefits of continuous SDLC and security integration

In order to be cost-effective and optimally functional, information security should be incorporated into the SDLC/EPLC at every stage from a system's original conception to its retirement. The integration of security requirements at the earliest stages of a system's life cycle promotes:

- Early identification and mitigation of security vulnerabilities and misconfigurations
- Better awareness of potential engineering challenges caused by mandatory security controls
- Identification of shared security services and re-use of security strategies and tools Informed executive decision-making through comprehensive risk management
- Documentation of important security decisions made during development
- Improved organization and customer confidence to facilitate adoption and usage as well as governmental confidence to promote continued investment