



Secure Software Development Lifecycle (SSDLC)

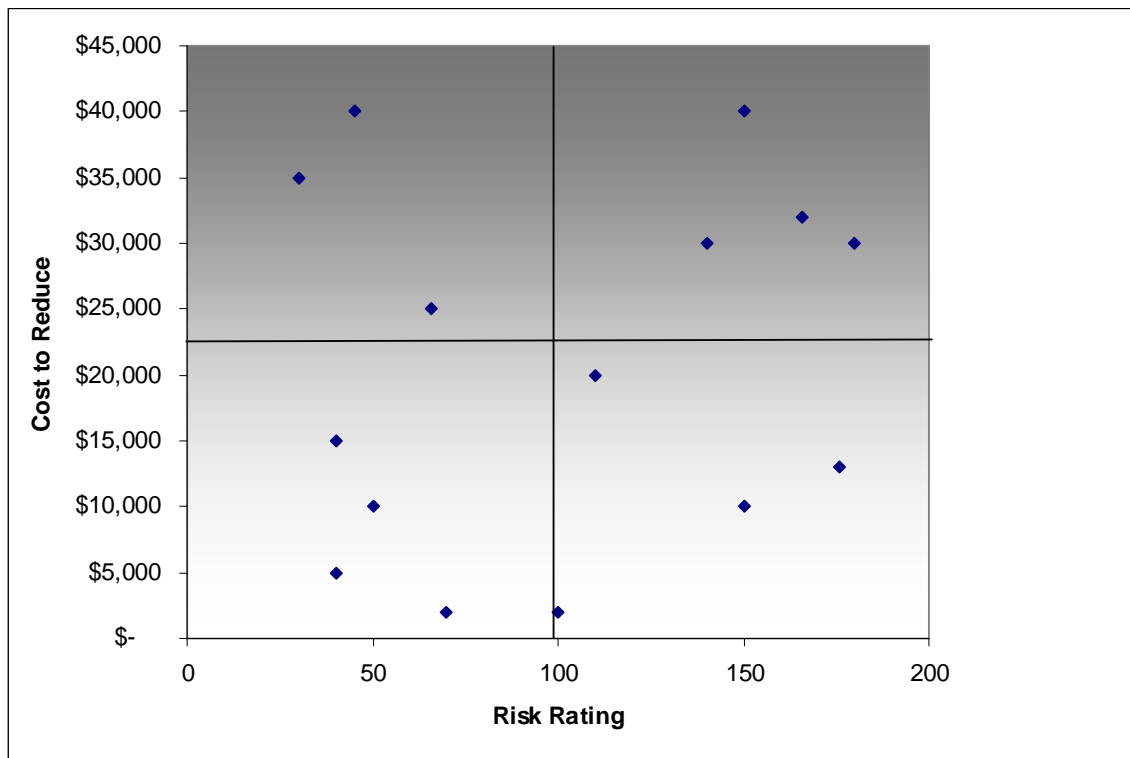
An SSDLC is a software development process based on application security principles adhering to a recognized standard and information privacy. It includes activities designed to ensure compliance to the standard and requires security-related steps in application development procedures.

Implementing an SSDLC lowers security risk and is part of a total Defense in Depth strategy.

Integral Business Solutions implemented an SSDLC process for its applications being developed for the U.S. Air Force. The metrics gathered through the implementation of this process were a key element in assessing the effectiveness of the effort. Integral's approach to gathering these metrics is highlighted below.

Prior to implementation Integral ran the existing applications through an application vulnerability scanning tool and performed an analysis of the results to create a risk posture for the application. Integral then applied Integral's Secure Agile Methodology (ISAM) processes to this analysis and in the next phases of development and remediation of the discovered vulnerabilities.

Each vulnerability was evaluated and ranked by impact, liability, and likelihood of the threat. $(\text{Impact} + \text{Liability}) * \text{Likelihood} = \text{Risk Rating}$. This risk rating and the cost to remediate were then used to create a chart for recommending action.



Lower Left = Low Risk and Low Cost – Recommend Fix
Lower Right = High Risk and Low Cost – Recommend Fix
Upper Left = Low Risk and High Cost – Recommend Evaluate
Upper Right = High Risk and High Cost – Recommend Schedule

Based on these recommendations, fixes and new feature development was prioritized and scheduled over a 6 month timeframe. During this period Integral implemented systematic changes to our process and procedures to improve our Risk Rating.

Systematic changes included:

- Educating our staff
- Implementing peer reviews
- Automated scan tools
- Automated continuous integration builds
- Automated regression testing
- Checkpoints throughout the development cycle to inspect the code and design looking for potential vulnerabilities and determining solutions

What resulted was a lowering of the risk posture to an acceptable level of risk for the client and a continuing effort to prevent new vulnerabilities from entering code during the maintenance phase for the system.



Our client chose to repair the risks in the right quadrants and some of the vulnerabilities in the left quadrants. During continued development most vulnerabilities that are identified have a lower risk rating and, since they are discovered earlier in the life cycle, are less expensive to remediate with costs often absorbed through normal development.

While the overall quality and security posture of the applications improved through the implementation of the SSDLC process, the greatest single impact has been the effect that SSDLC thinking has had on Integral's development culture. Awareness of application security concepts and specific application vulnerabilities enhanced our development team's collaboration and ability to mitigate security risks.