

Open Security Architecture: Comparing SSDLC

NIST 800-64-Rev2	Initiation - Business Impact - Privacy Considerations - Define Control Gates	Development - Analyze Risks - Analyze Security Ctrls - Define Security Architecture - Engineer in security Controls - Test - Document	Implementation / Assessment - Integrate security into environment - Test and assess - Certify and accredit	Operation / Maintenance - Change management - Continuous monitoring - Recertification - Testing - Accreditation - Continuous monitoring	Disposal - Ensure Information Preservation - Sanitize media - Dispose hw - Reuse SW licenses
	Source: http://csrc.nist.gov/publications/PubsSPs.html Strength: defined outputs for each step, defined dependencies between steps, well summarized and visualized				

MS SDL	Training Core training	Requirement - Analyze security and privacy risks - Define quality gates	Design - Threat modelling - Attack surface analysis	Implementations - Specify tools - Enforce banned functions - Static Analysis	Verification - Dynamic / Fuzz testing - Verify threat models / attack surface	Release - Response plan - Final security review - Release archive	Response - Response execution
	Source: http://msdn.microsoft.com/en-us/magazine/dd153756.aspx Strength: practical and tool supported						

OWASP CLASP mapped on MS SDL	Training Institute security awareness program Identify global security policy Identify user roles and resource capabilities	Requirement Implement and elaborate resource policies and security technologies Annotate class designs with security properties Identify attack surface Detail misuse cases Document security-relevant requirements Identify resources and trust boundaries	Design Research and assess security posture of technology solutions Perform security analysis of system requirements and design (threat modeling) Specify database security configuration Apply security principles to design Specify operational environment	Implementations Implement interface contracts Integrate security analysis into source management process	Verification Identify, implement and perform security tests Perform source-level security review	Release Build operational security guide Perform code signing Verify security attributes of resources	Response Manage security issue disclosure process Address reported security issues Monitor security metrics
	Clasp Source: http://www.owasp.org/index.php/Category:OWASP_CLASP_Project Strength: mapping of activities to roles						

Gary Mc Graw	Requirements & Use Cases Abus Cases Security Requirements Risk Analysis	Architecture and Design Risk Analysis	Test Plans Risk-based security tests	Code Code review (tools)	Tests and Test Results Risk analysis and penetration testing	Feedback from the field Security Opeartions
	Source: http://books.google.com/books?id=HCQdypbpZXgC&dq=inauthor:Gary+inauthor:McGraw&ei=TxagSdeHCPW6M4_30YoC Strength: risk driven					