

OSA SDLC: Core controls for secure solution development

	Training	Requirement	Design	Implementation	Verification	Release	Response
Application Owner	Business process Essentials	Strategic risk analysis Privacy policy SLA definition	Role and permission design				Service Level Management
Project manager		Project risk analysis					
Analyst		Solution risk analysis	Abuse case definitions	Analysis of coverage of automated tests			
SW and Infrastructure Architect		Technology risk analysis	Capacity planning Disaster recovery Planning		Verify SLA fulfillment capabilities		
SW Engineering		Technology prototyping		Code review Static source analysis	Verify abuse cases		
QA Engineering	Process framework	Define quality gates			Automated black box and white box testing	Verify claimed security attributes and sign-off release	
Security Specialist	Secure development Principles Security policy	Security requirements elicitation Attack surface identification Define trust boundaries	Security design review Threat modelling		Penetration testing	Response plans as part of operational security guide	Security Incident Management
Operations							Change Management (incl. Vulnerability Management) Continuos Monitoring

Definitions:

Solution risk	A risk posed by the deployed solution to the business that it serves or to other stake holders
Project risk	A risk that threatens the goal of the project (which is put in place to develop the solution)
Penetration testing	A manual testing process that requires knowledge of potential vulnerabilities