Integrating Information Assurance into Agile and Rapid Technology Development

Agile IA

Kathy McGinn, Marine Corps Systems Command
Monica Nelson, Marine Corps Systems Command
Dale Daigle, Space and Naval Warfare Systems Command

Abstract. In this paper we present a method for integrating information assurance requirements into agile and rapid technology development. This integrated approach advocates involvement of the information assurance expert at the onset of system development and design—building requirements in proactively. The focus is on collaboration, continuous monitoring, and leveraging automated testing for formal validation.

Introduction

As "agile" software development becomes more common in government and industry, it poses a challenge: integrating Information Assurance (IA) into system requirements and the development process. How do we take a gate-styled serial process, segment it into increments, and then integrate it? How do we move IA requirements from right to left in the development schedule, instead of tacking them onto the end? How do we document that process incrementally and obtain acceptance of the security posture by the approval authority? At Marine Corps Systems Command, the Information Assurance Management Team supporting Program Manager Marine Intelligence has developed an integrated information-assurance process, called "agile IA," to address these issues and better support agile software development.

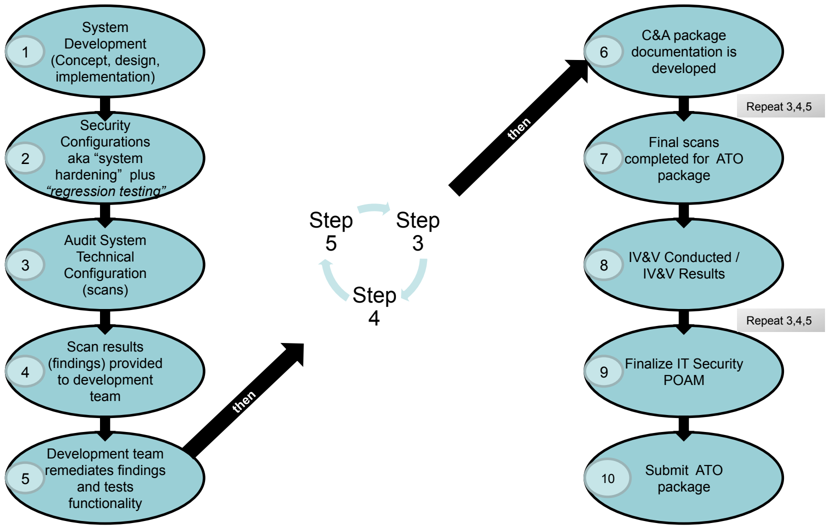

1
System Development (Concept, design, implementation)
2
Security Configurations aka "system hardening" plus "regression testing"
3
Audit System Technical Configuration (scans)
4
Scan results (findings) provided to development team
5
Development team remediates findings and tests functionality
then
Step 3
Step 4
Step 5
then
6
C&A package documentation is developed
Repeat 3,4,5
7
Final scans completed for ATO package
8
IV&V Conducted / IV&V Results
Repeat 3,4,5
9
Finalize IT Security POAM
10
Submit ATO package

Figure 1: Legacy serial process of system development and preparation

Typically, legacy certification and accreditation practices assess IA requirements after a system has been designed and developed, generally through serial processes that prolong the development schedule. This results in reactionary implementation of security configurations and creates a cascading effect of schedule slips and unplanned costs. This traditional approach can leave both technical and administrative security requirements inadequately addressed. It frequently overlooks operations security—even core requirements such as ensuring that personnel are properly cleared.

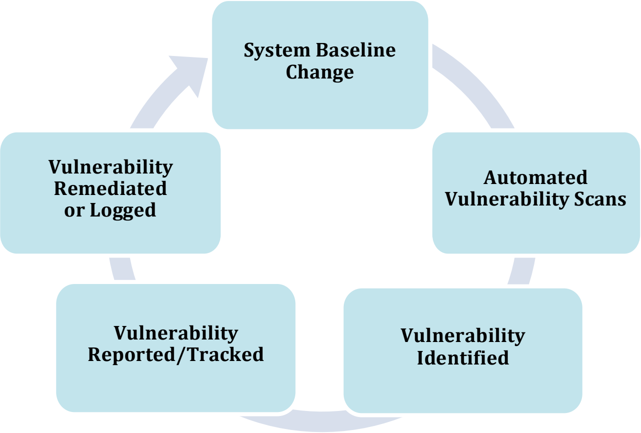
Legacy processes involve cycles of configuration known as system "hardening." The cycle consists of scanning, remediating, rescanning and reconfiguration, in multiple iterations whose goal is to minimize vulnerability. The baseline must be maintained while the system is documented and formal, Independent Verification and Validation (IV&V) is conducted. IV&V likewise involves cycles of activity that must occur while other processes are accomplished for Certification and Accreditation (C&A). The combined process of hardening and IV&V can take anywhere from 12 to 24 months—occasionally even longer.

Figure 1 depicts the average legacy serial process of preparing a system for obtaining authority to operate. Typically, the IA subject matter expert, such as the information-system security manager or information system security engineer, is called into the effort at step 3.

The goal of system development is to deliver a capability to an end user—in the case of the U.S. Marine Corps, to the warfighter. But legacy practices delay delivery, and for some systems—such as intelligence sensor systems—delay is itself a security risk. As stated in a recent paper by the SEI at Carnegie Mellon University, "the information assurance accreditation delay is so extensive (often months to a year) that [the gated implementation method of] the DIACAP process almost negates the benefits gained through rapid development methods."[1]

Collaborate, Integrate, Automate

The integrated or "agile IA" approach encourages a rapid, flexible response to vulnerabilities that emerge as the system is developed. The key difference between agile IA and the legacy approach is the integration of security at the onset of system development, allowing proactive attention to requirements. The IA subject-matter expert is involved in development from day one, and is part of the agile development team, which addresses and prioritizes IA requirements during sprint planning. Automated scanning, which includes automated code-review tools, allows the expert to monitor the system continuously as it is being developed. As security requirements are identified, they are reported in the information-technology security plan of actions and milestones. By "baking" security into the product, agile IA reduces security risk at any point in development and minimizes redundancy in the hardening process. Figure 2 reflects the cycle of continuous monitoring and proactive remediation and tracking.



System Baseline Change
Automated Vulnerability Scans
Vulnerability Identified
Vulnerability Reported/Tracked
Vulnerability Remediated or Logged

Figure 2 – Continuous monitoring and remediation tracking process

C&A also poses the usual timeline challenges. In the agile approach, artifacts are created incrementally as the system develops. IA controls are documented as the information becomes available. Documentation is limited to the minimum required to satisfy the approving authority requirement to depict the system security posture.

Lastly, and more significantly, a certified validator is engaged to leverage the results of the continuous monitoring already occurring during each sprint. This enables the validator to leverage the test results for formal validation and verification, and perform a shortened "hybrid" style of IV&V. The formal IV&V event is reduced to minimally disruptive administrative checks and audits, obviating the intensive auditing that typically interrupts system development. System development is allowed to continue during the IV&V audit.

Figure 3 depicts how continuous monitoring can be tracked to reflect the changing baseline of a system given its vulnerability findings. Note that in the beginning of the monitoring, the number of findings is high. As the system is developed and remediation occurs, findings are reduced. However, fluctuations in the baseline should be expected as system requirements are added.

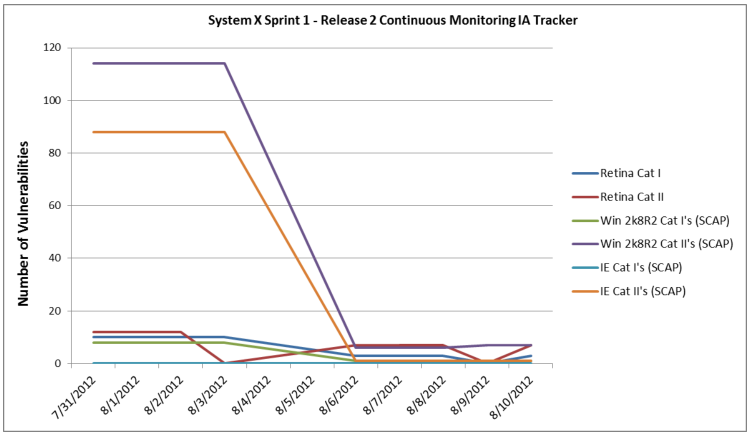


Figure 3 – Continuous monitoring scan results example

Conclusion

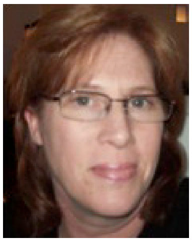
Integration of security configuration requirements at initial stages of system development eliminates the legacy practice of reactionary IA implementation. Introducing IA expertise at the onset of development provides a more holistic approach to identifying and implementing security requirements. The agile IA approach can be implemented within other development methods and should not be practiced for agile development alone. It allows an incremental and controlled approach for IA implementation and ensures a more secure posture of a capability or product release. Figure 4 depicts a sprint timeline with concurrent activities per sprint to include security configuration, functional testing, continuous monitoring, formal auditing, and incremental C&A package creation.

Integrated IA will reduce the schedule slippage and unplanned costs that are inherent when IA is bolted on at the end of system development. It will also reduce redundancy in system-hardening processes, leverage auditing activity for multiple purposes, and produce an artifact package that more quickly depicts the system's security posture. More importantly, it will ensure that capabilities or products provided to the warfighter are less vulnerable to exploitation.

NOTES

1. Bellomo, Stephany; Woody, Carol, Software Engineering Institute at Carnegie Mellon, Paper: DOD Information Assurance and Agile: Challenges and Recommendations Gathered through Interviews with Agile Program Managers and DOD Accreditation Reviewers, Technical note CMS/SEI-2012-TN-024

ABOUT THE AUTHORS



Kathy McGinn is the lead Information System Security Manager for the Marine Intelligence program office at the Marine Corps Systems Command in Quantico, Virginia. She currently serves as an IA subject matter expert; managing certification and accreditation requirements for multiple programs. She has extensive knowledge and experience in information assurance process development and certification and accreditation. She is a certified information systems security professional (CISSP).

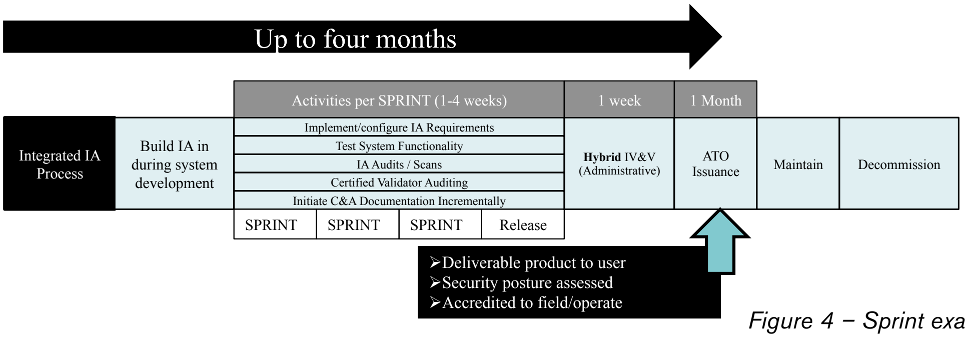
E-mail: kathy.mcginn@usmc.mil

Monica S. Nelson is an Information System Security Manager for the Marine Intelligence program office at the Marine Corps Systems Command in Quantico, Virginia. She currently serves as the "agile IA" subject matter expert for her team. She has extensive knowledge and experience with agile software development and is a member of the team that developed the first integrated information assurance process using Agile methodologies. She holds the CompTIA Security+ certification and has a Bachelor's degree in Decision Science and Management Information Systems from George Mason University.

E-mail: monica.nelson@usmc.mil

Dale Daigle is the lead Information System Security Engineer (ISSE) for Distributed Common Ground/Surface System - Marine Corps (DCGS-MC) at Space and Naval Warfare Systems Command (SPAWAR) in Charleston, South Carolina. He currently serves as a subject matter expert on Information Assurance (IA) and "Agile IA" for DCGS-MC. He has extensive knowledge and experience with IA and agile software development and led efforts to develop the first integrated IA process using Agile methodologies. He is a Certified Information Systems Security Professional (CISSP).

E-mail: dale.daigle@navy.mil



Up to four months

Activities per SPRINT (1-4 weeks)

1 week

1 Month

Integrated IA Process

Build IA in during system development

Implement/configure IA Requirements

Test System Functionality

IA Audits / Scans

Certified Validator Auditing

Initiate C&A Documentation Incrementally

SPRINT

SPRINT

SPRINT

Release

Hybrid IV&V (Administrative)

ATO Issuance

Maintain

Decommission

➢Deliverable product to user
➢Security posture assessed
➢Accredited to field/operate

Figure 4 – Sprint example with concurrent integrated activity