Proposed Cyber Test and Evaluation Process across the Software Development Lifecycle

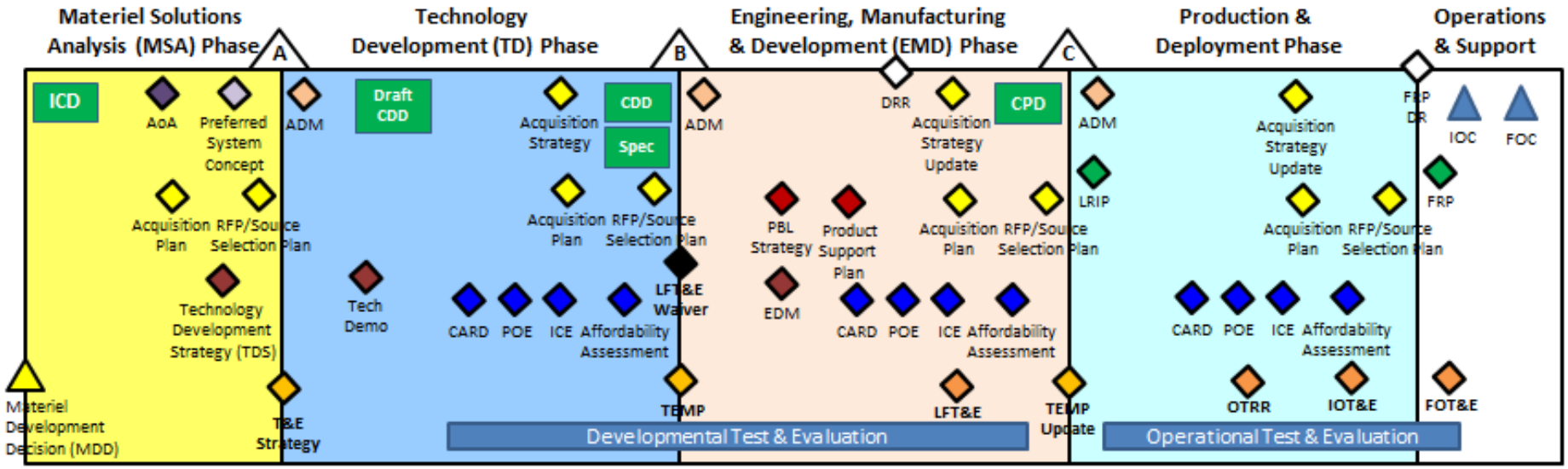
Carolyn R. Keith
MSIA, CISSP-ISSEP, CISA, CTEP
November 2013
ITEA 30th Annual Symposium

TASC
INSIGHT APPLIED™

Introduction

- DDT&E suggestion
  - Shift-Left for Cyber Security Testing
  - Current cyber threat requires better and cheaper security solutions
- Response
  - Move initial Cyber Security Testing activities earlier in the Software Development Life Cycle (SDLC)
  - Test Cyber Security throughout the entire SDLC

DOD Acquisition Life Cycle



Pre-Phase A Reviews
- Alternative Systems Review
- Initial Technical Review

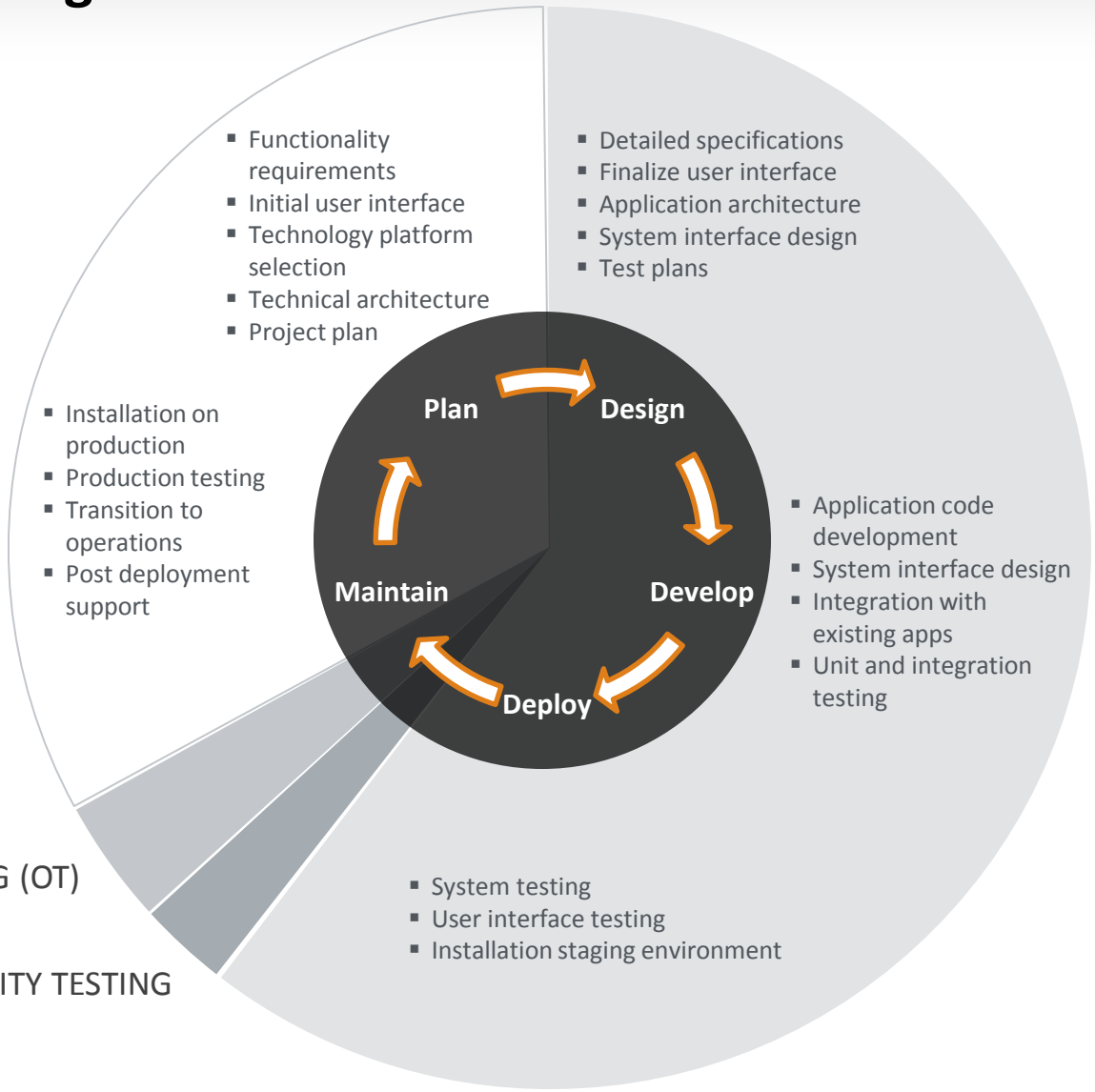
Phase A Reviews
- System Requirements Review
- System Functional Review
- Preliminary Design Review
- Technology Readiness Assessment
- Integrated Baseline Review

Phase B Reviews
- Integrated Baseline Review
- Critical Design Review
- Test Readiness Review
- Flight Readiness Review
- System Verification Review
- Functional Configuration Audit
- Production Readiness Review
- Technology Readiness Review

Phase C Reviews
- Integrated Baseline Review
- Operational Test Readiness Review
- Physical Configuration Audit

Full Scale Framework

Security Testing



Issue

Cost of Fixing Vulnerabilities Later

Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
Requirements		$139	
Design		$455	
Coding		$977	
Testing	50	$7,136	$356,800
Maintenance	150	$14,102	$2,115,300
Total	**200**		**$2,472,100**

Source: www.cert.org

Cost of Fixing Vulnerabilities Early

Stage	Critical Bugs Identified	Cost of Fixing 1 Bug	Cost of Fixing All Bugs
Requirements		$139	
Design		$455	
Coding	150	$977	$146,550
Testing	50	$7,136	$356,800
Maintenance		$14,102	
Total	**200**		**$503,350**

TASC

Response

- Pre-Milestone A
  - Perform a Security Risk Assessment
  - Conduct Threat Modeling
  - Execute a Tabletop Contingency Exercise
  - Execute a Hypothetical Penetration/Exploitation Exercise

Response (continued)

- Pre-Milestone B
  - Add Granular Security Requirements to Critical Design Documents
  - Conduct “Hack the Design” reviews

Response (continued)

- Pre-Milestone C
  - Perform Code Reviews Earlier and Continuously
  - Apply STIG and Current Information Assurance Vulnerability Management (IAVM) Notice Requirements to the Code and Applications
  - Incorporate Vulnerability Scanning and Security Fix or Mitigation Activities
  - Initiate Penetration Activities Earlier
  - Change the mindset - Authorization to Operate (ATO) is not the end of operational security, it is the beginning…

Response (continued)

- Deployment Phase
  - Continue to apply STIGs and IAVM notices
  - Perform final Code Review
  - Continue Vulnerability Scanning
  - Execute a full Penetration/Exploitation Test
- Maintenance Phase
  - Continue to apply STIGs and IAVM notices
  - Continue Vulnerability Scanning
  - Execute random, unannounced Penetration/Exploitation Tests

Summary

	Activity	Plan	Design	Develop	Deploy	Maintain
Historical Schedule	Security Risk Assessment			●		
	Threat Modeling		●			
	Security Penetration Exercise				●	●
	Contingency Tabletop Exercise					●
	Security Design			●		
	Security Code Reviews				●	
	Implement STIGs and IAVAs				●	●
	Vulnerability Scanning and Security Reviews				●	●
Proposed Schedule	Risk Assessment	●				
	Threat Modeling	●				
	Security Penetration Exercise	●		●	●	●
	Contingency Tabletop Exercise	●			●	●
	Security Design	●	●			
	Security Code Reviews		●	●	●	
	Implement STIGs and IAVAs		●	●	●	●
	Vulnerability Scanning and Security Reviews			●	●	●

TASC

Questions


TASC
INSIGHT APPLIED™