Authority-to-Operate – Navigating DoD Cybersecurity Compliance

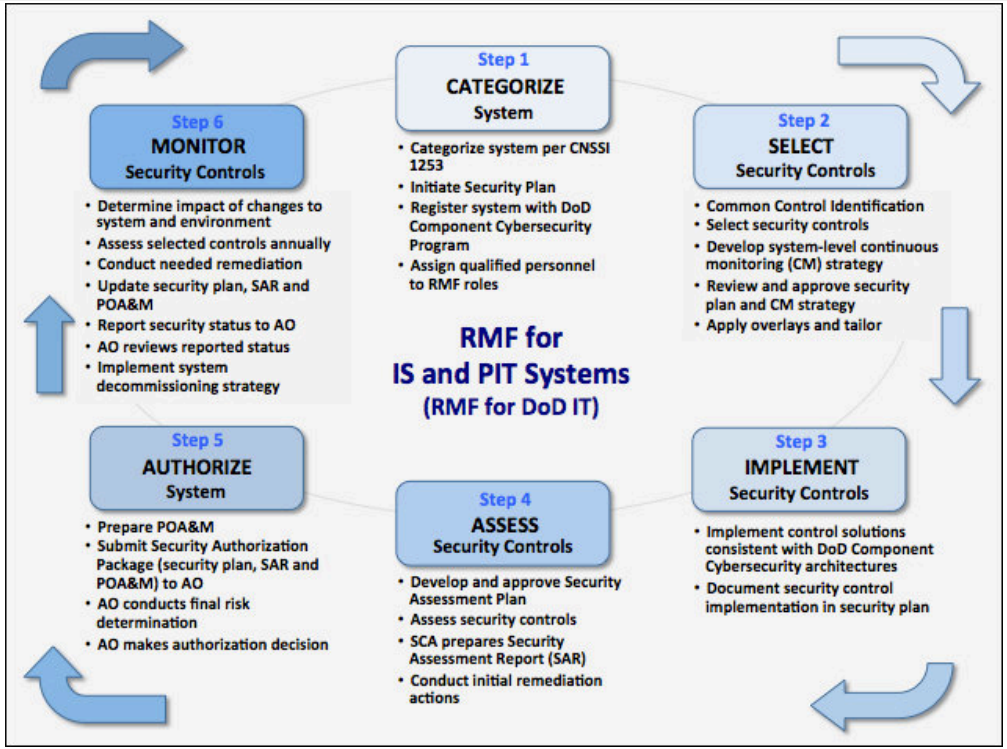
Don Lawson

Andrew Maxon

IA Threats

- Internal
  - 60% of all attacks happen from the inside
  - Disgruntled employees, spies, or terrorists
  - Unintentional damage
    - This is the largest internal threat as either due to poor training or not following procedure has led to deletion of files and
- External
  - Crackers, terrorist groups, foreign countries, and protesters
  - In 2013 the US the Pentagon acknowledged it is scanned or attacked more than 10 million times a day.
  - Similarly, in 2013 the state of Utah faces 20 million attempts per day, up from 1 million a day two years earlier

RMF Process


Step 1
CATEGORIZE
System
• Categorize system per CNSSI 1253
• Initiate Security Plan
• Register system with DoD Component Cybersecurity Program
• Assign qualified personnel to RMF roles
Step 2
SELECT
Security Controls
• Common Control Identification
• Select security controls
• Develop system-level continuous monitoring (CM) strategy
• Review and approve security plan and CM strategy
• Apply overlays and tailor
Step 3
IMPLEMENT
Security Controls
• Implement control solutions consistent with DoD Component Cybersecurity architectures
• Document security control implementation in security plan
Step 4
ASSESS
Security Controls
• Develop and approve Security Assessment Plan
• Assess security controls
• SCA prepares Security Assessment Report (SAR)
• Conduct initial remediation actions
Step 5
AUTHORIZE
System
• Prepare POA&M
• Submit Security Authorization Package (security plan, SAR and POA&M) to AO
• AO conducts final risk determination
• AO makes authorization decision
Step 6
MONITOR
Security Controls
• Determine impact of changes to system and environment
• Assess selected controls annually
• Conduct needed remediation
• Update security plan, SAR and POA&M
• Report security status to AO
• AO reviews reported status
• Implement system decommissioning strategy
RMF for
IS and PIT Systems
(RMF for DoD IT)

IA Implementation Strategies

Engineered Cybersecurity (Baked In)

The process of integrating an IA engineer into the system's multiple integrated product teams (IPTs) from the start

- Budgeted from beginning
- Less expensive
- Part of the security engineering process
- Smoother C&A effort
- Easier to leverage
- More secure system

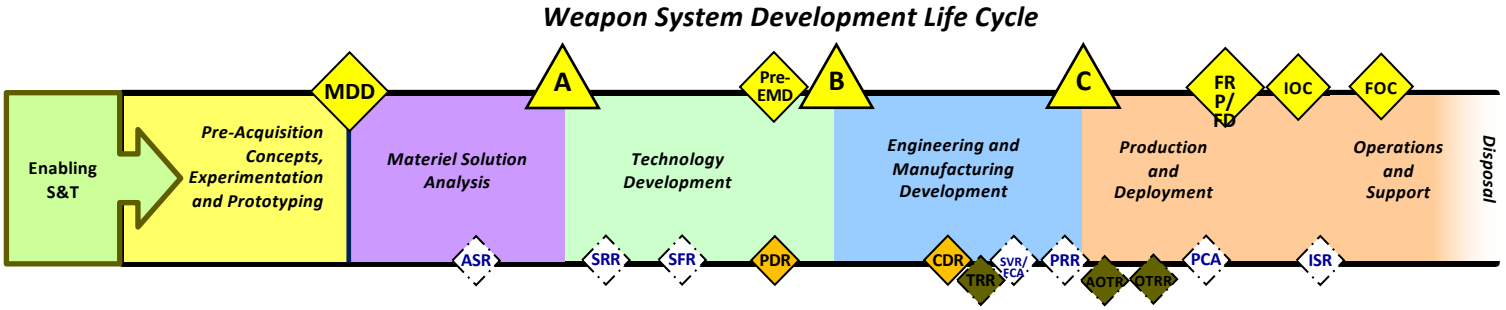
vs.

Enhanced Cybersecurity (Bolted On)

The process of adding security to a legacy or ready-to-be-fielded system

- More expensive
- Security can damage systems not designed for security
- Not a preferred method
- Less secure system

Government Acquisition Process



AOTR - Assessment of Operational Test Readiness
ASR - Alternative Systems Review
CDR - Critical Design Review
EMD - Engineering and Manufacturing Development
FCA - Functional Configuration Audit
FD - Full Deployment
FOC - Full Operational Capability
FRP - Full-Rate Production
IOC - Initial Operational Capability
ISR - In-Service Review
MDD - Materiel Development Decision
OTRR - Operational Test Readiness Review
PCA - Physical Configuration Audit
PDR - Preliminary Design Review
PRR - Production Readiness Review
S&T - Science and Technology
SRR - System Requirements Review
SFR - System Functional Review
SVR - System Verification Review
TRR - Test Readiness Review

Mandatory technical reviews

Best practice technical reviews and audits

Test reviews (see DAG Chapter 9)

What to look out for?

- Security Requirements Review (SecRR) – Don't get saddled with Government Responsibilities
- PDR & CDR – Take in to account cost saving endeavors your customer will agree with
- From CDR through CPI and GFI – Develop on Cyber Secure Baselines, fix issues early
- GFI/JFI/CGFI – Contractor/ Government / Joint Final Inspection, final test system requirements test

Certification Documentation

Deliverable	Name	Description
SIP	System Identification Profile	Contains detailed system information, points of contact, and, specific Cybersecurity information
IP	Implementation Plan	Details all applicable Cybersecurity controls contained in DoD 8500.2 and Government Agency C&A Guide. The IP will list the Cybersecurity controls as applicable, not applicable, site or inherited with further details.
SSP	System Security Plan	Details how the Cybernet Cybersecurity process will protect the system through its security lifecycle.
POA&M	Plans of Action and Milestones	A plan and schedule of any issues that are found during the C&A effort. Lists all technical and programmatic risks associated with vulnerabilities discovered during testing. This report will be classified <CLASSIFICATION>.
Scorecard	Scorecard	Details of security and C&A compliance for the system(s).
False Positives	False Positive Report	Details the findings found that are false detections.
Test Plan	Test Plans and procedures	Test steps and procedures that are used to validate security of the system(s) including: scans, security reviews, and individual validation tests
Validation Report	Validation Report, Scan Results/Test Results	Pass/Fail and detailed descriptions and results of each test step.
Checklist and SRRs	STIG Checklists and Security Requirement Reviews	The checklists and reviews that were used to ensure that all security measures were installed.
IAVM Plan	Information Assurance Vulnerability Management Plan	This is the plan of how the systems security posture will be managed throughout its lifecycle.
Inherited Findings	Inherited Findings report	Details the controls that are inherited and where they are inherited from.
RMF Artifacts	Artifacts of the RMF process	Includes ACAS/Nessus data files, SRR reports, SCAP results, C&A Signature Page, Contingency Plan, Contingency Plan Signature page, CMP, IRP, Interconnections Artifact, STIG Compliance and any additional information required for a successful C&A process.

Recap

- DoD uses NIST guidelines to protect against cyber threats
- You want to bake cyber in to your designs rather than try to bolt it on later
- Have personnel in your SecRR that can navigate controls and responsibility
- Engineer cyber in from the start to eliminate re-engineering costs
- Always test your software on cyber secured baselines to isolate issues early