



# A Systems Engineering approach to applying Risk Management Framework (RMF) for a successful program and a secure system – a case study

RMF is Not a 4-Letter Word

**Craig Covak**

*Lockheed Martin Rotary & Mission Systems (RMS)  
Cybersecurity Functional Area Manager  
[Craig.Covak@lmco.com](mailto:Craig.Covak@lmco.com)*

**Michael Coughenour**

*Lockheed Martin Rotary & Mission Systems (RMS)  
System Engineering Technologist  
[Mike.Coughenour@lmco.com](mailto:Mike.Coughenour@lmco.com)*

DISTRIBUTION STATEMENT A. Approved for Public Release 16-MDA-8871  
(30 September16). Distribution is unlimited.



# Overview

---

- What it is...
- What it is not...
- BE SECURE – 6 Steps
- Essential structure of RMF
- Systems Engineering Approach to RMF
- RMF Execution – Action Plan
- Command & Control, Battle Management, and Communications (C2BMC) – Joint Execution Process
- Parting Gems of Wisdom
- Credit where credit is due



# What it is...

- RMF – Risk Management Framework
  - New Accreditation (a.k.a. Authorization) construct
  - Manage security risk at acceptable level
  - More complex, much more granular
    - Case study: 18 control families » 512 controls » 1927 Control Correlation Identifiers (CCIs)
- frame·work (*noun*) – Basic structure supporting a system...to manage risk (security)
- Confidentiality, Integrity, Availability
  - High – Medium – Low categorization for each tenet
    - Case study: H-H-H Classified system

Compliance evaluation of all CCIs required for final Authorization decision



# What it is NOT...

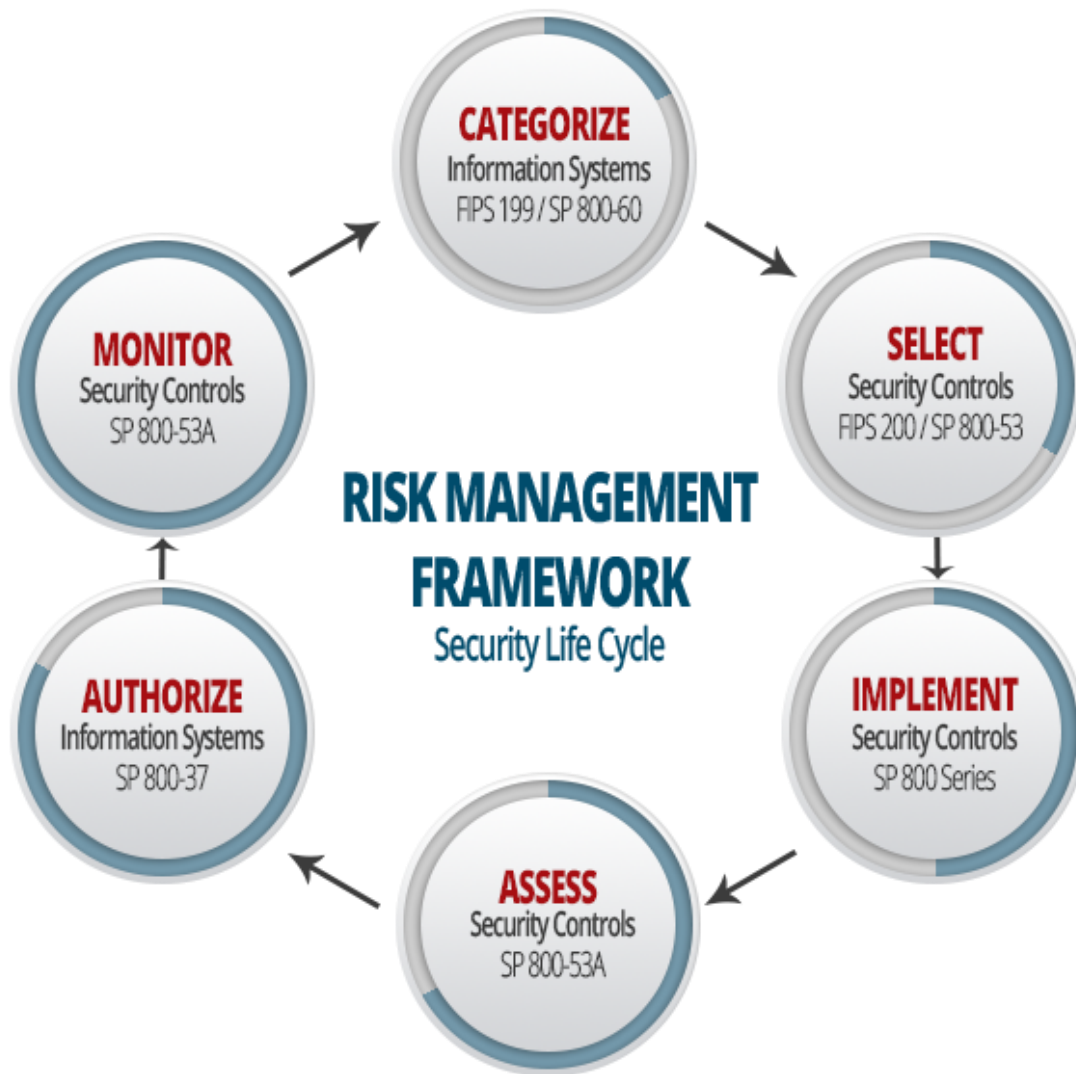
---

- pro·cess (*noun*) – a series of actions or steps taken in order to achieve a particular end
- DoD Information Assurance Certification and Accreditation Process (DIACAP) redefined
  - A System Accreditation
- A Cyber issue
  - RMF is a system-wide issue
  - Involves all Functional Areas (FAs)
    - Ex: Development, Networks, Systems Engineering, Operations & Maintenance, Program Management Office, Cyber
- A 4-letter word



**If you don't want to  
avoid the pitfalls of  
securing your system  
feel free to leave now...**

# 6 Steps – BE SECURE





# Essential Structure of RMF

- System Categorization (e.g., Confidentiality, Integrity, Availability)
- Selection & assignment tailoring
- Control families » controls » control enhancements » CCIs (~2000)

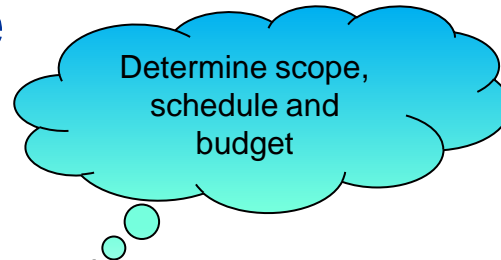
## Control Families

- Access Control (AC)
- Awareness and Training (AT)
- Audit (AU)
- Security Assessment (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Incident Response (IR)
- System Maintenance (MA)
- Media Protection (MP)
- Physical and Environmental (PE)
- Security Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- Risk Assessment (RA)
- System Acquisition (SA)
- System Communications (SC)
- System Integrity (SI)

# SE Approach – Project Planning

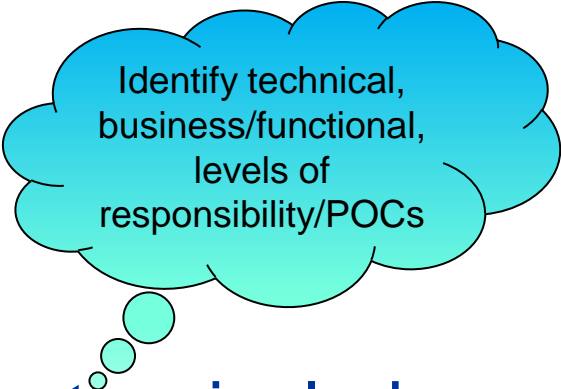
---

- It's Imperative to get management and key stakeholders buy-in to initiate RMF execution
- In order to successfully execute RMF for a system, a program needs to consider the entire development lifecycle
- This lifecycle begins with a solid plan that encapsulates FA team members that take into account the policy, engineering, development, testing, fielding, and sustainment efforts involved for RMF execution





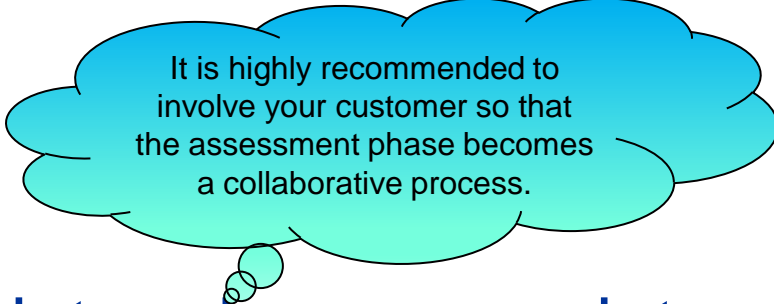
# SE Approach – Requirements Definition

- Once the plan has been baselined, the engineering effort should be initiated with the longest lead time items - system specification requirements
- 
- A light blue thought bubble with a black outline, containing the text 'Identify technical, business/functional, levels of responsibility/POCs'. It is connected to the main list by three smaller circles of decreasing size.
- Identify technical, business/functional, levels of responsibility/POCs
- A few things to take into consideration include:
    - Sunset old DIACAP requirements
    - Traceability to enterprise (higher-level) specifications, policies
    - Determining appropriate level for system specification requirements (controls vice CCIs)

# SE Approach – Design & Development

---

- As requirements are finalized, the engineering effort should continue with determination of approach & scope of effort for each RMF CCI
- This control determination flows down to FA assessment of each CCI as there is a one-to-many relationship

A light blue thought bubble with a black outline and a small tail pointing towards the bottom left. It contains the following text:

It is highly recommended to involve your customer so that the assessment phase becomes a collaborative process.

- Assessment should determine appropriate stakeholders necessary to implement RMF for the program / system



# RMF Execution – Action Plan

---

## 1. Analysis

- Controls Determination
- Implementation Plan

## 2. Assessment

- CCI assigned to appropriate FAs for action
- RMF CCI spreadsheet estimates from each FA

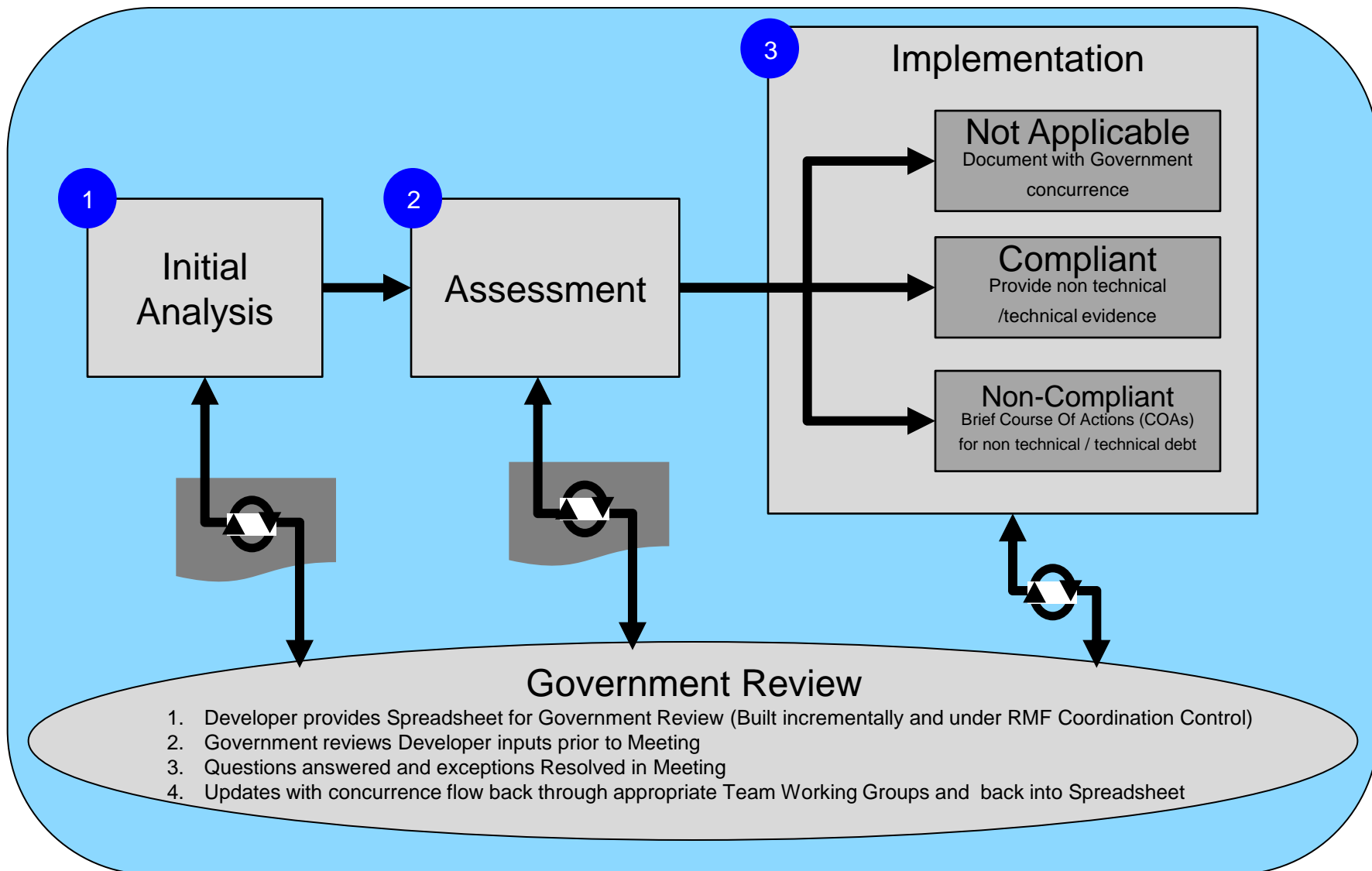
## 3. Implementation

- CCI incorporated into applicable artifact(s)
- System Modification Requests (SMRs) for Element Specification (ES) requirements tested

**Control / CCI Burndown required for each execution step**



# Joint Execution Process





# Parting Gems of Wisdom

- A systems engineering approach will set the program on a good trajectory for successfully executing RMF
- These are a few lessons that we have learned upon embarking upon this journey to successfully execute RMF for C2BMC:
  - Get others involved early and often
  - Do not be afraid to chip away at the problem
  - Iterations are necessary while moving through the lifecycle
  - Take it one control family at a time
  - Start today...no better time than the present

More are given in the detailed presentation 15:45 this afternoon



# Credit where credit is due

---

- C2BMC Program
- Missile Defense Agency (MDA) / Engineering (BCE) Organization
- Lockheed Martin
  - C4USS – C4ISR & Undersea Systems
  - RMS – Rotary and Mission Systems
- Team Mates
  - Lockheed Martin
  - Boeing
  - General Dynamic
  - Northrop Grumman
  - Raytheon