LOCKHEED MARTIN
BOEING
GENERAL DYNAMICS
NORTHROP GRUMMAN
Raytheon

Bridging the ABYSS– Transitioning An In-Motion Development Program From DoD Information Assurance Certification and Accreditation Process (DIACAP) to Risk Management Framework (RMF)

A Case Study of Changing the Tires on the Bus While Moving

Michael Coughenour
Lockheed Martin RMS,
System Engineering Technologist
Mike.Coughenour@lmco.com

Craig Covak
Lockheed Martin RMS,
Cybersecurity Functional Area Manager
Craig.Covak@lmco.com

Be Secure – Its Important!

- Building security into a system of any significant complexity is tough enough in today's environment
- Getting the system accredited takes a lot of work

BUT

- Changing the rules in the middle of the game, though sometimes necessary, makes it REALLY tough!

Take a Lifecycle Approach for Program Success

- What the transition looks like is directly dependent on where your program is in its lifecycle when the transition begins
- If transitioning pre critical design review (CDR) – can be handled like a significant requirements/mission change
- Presentation & case study focus on transition after deployment of some of the capabilities

The Earlier the Better

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…

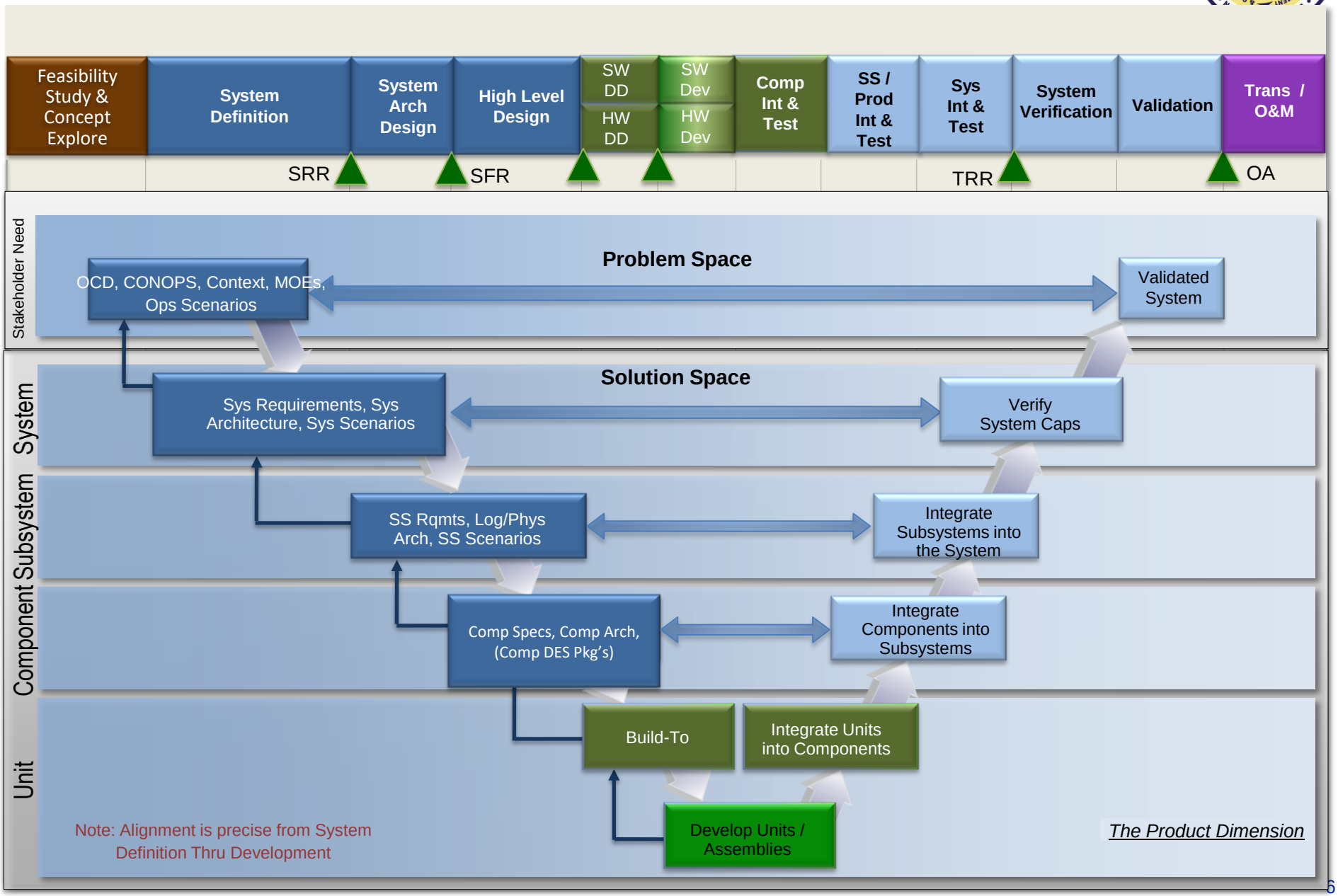
- pro·cess *(noun)* – a series of actions or steps taken in order to achieve a particular end

- DIACAP redefined
  - A System Accreditation

- A Cyber issue
  - RMF is a system-wide issue
  - Necessitates involvement from all Functional Areas (FA)
    - Ex: Dev, Net, Systems Engineering, O&M, Program Management Office, Cyber

- A 4-letter word

A Context – the System Development Lifecycle



CASE STUDY:
A LARGE MISSILE DEFENSE PROGRAM – COMMAND & CONTROL, BATTLE MANAGEMENT, AND COMMUNICATIONS (C2BMC)

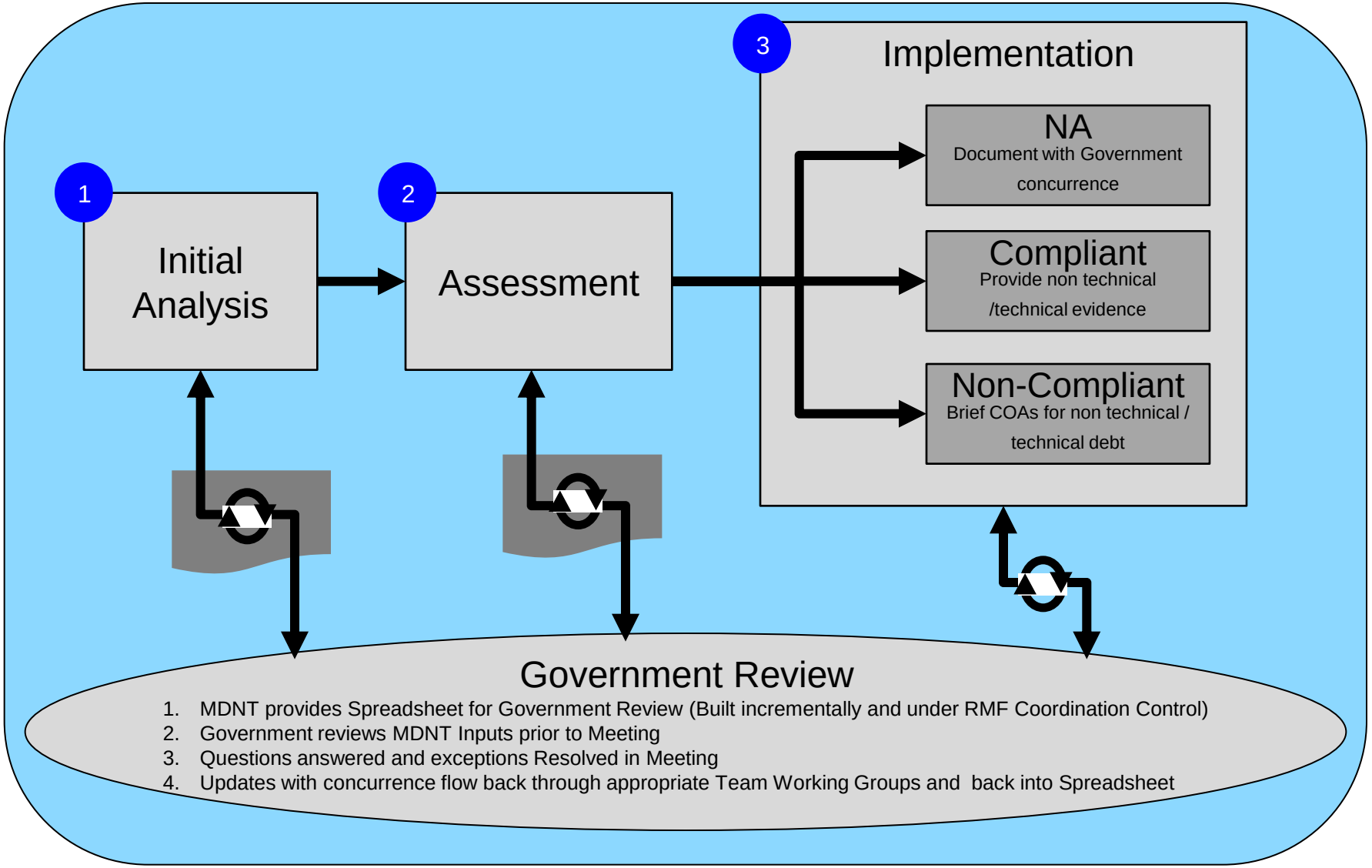
First Understand RMF (Dissecting It)

- The process wrapper
- Controls elaborated in CCIs
- Customer prioritization (critical/non-critical)
- Tech vs non-tech CCIs - proceed with caution
- Essentially - Tech CCIs become system reqts
- Have to deal with DIACAP-based sys reqts
  - Transform to RMF sys reqts or Create RMF baseline and retire/sunset DIACAP
  - Stuck between what is already done and what comes next – a look through the lifecycle

*Authorization to Proceed (ATO)

On the Path to ATO – Final Authorization Decision

Joint Execution Process



To the Heart – Gems of Wisdom

- Early in the Transition:
  - Help key decision makers understand the difference between DIACAP and RMF early
  - Define Key terms → helps broad-reaching decision early
    - "organization" is critical in determining which [org] should handle the CCI (Prgm Cmd, Dev Team/Org, or Ops/sust Cmd/Team)
    - Differentiate between "business" & "mission"
      - "Business" used predominately by non-DoD, "mission" by DoD
    - Differentiate between "function" & "capability"
      - Capability use at acquisition level and system process level
    - Accreditation → authorization – Goes to culture: give people time to make terminology shifts - use both to avoid confusion and lack of understanding the importance of, until confident the culture has shifted

To the Heart – Gems of Wisdom (cont.)

- Early in the Transition (cont.):
  - Build a map to all the relevant sources / resources and make sure all stakeholders involved in the analysis and assessment have access to them, particularly those not in public domain – e.g. “.mil”
  - Handle the level 1 (“-1”) CCIs up front (e.g. SA-1)
    - That context effects all subsequent CCIs in the family

To the Heart – Gems of Wisdom (cont.)

- Interpretation is the lynchpin – and the most difficult to run to ground
- Work on CCIs as a Group not independently (e.g. by family / enhancement)
  - CCIs are essentially dissections of 800-53 controls into atomic pieces – start in 800-53 to begin "understanding" context and intent
  - E.g CM-5 - *The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system* became 8 CCIs

To the Heart – Gems of Wisdom (cont.)

Two particularly big challenges

- Develop Approach to and Get agreement thru entire Lifecycle for sell-off of CCIs/requirements accomplished before transition – i.e. Functionality implemented under DIACAP

- Culture is a powerful force – it must not be ignored! It must be assessed and accounted for in the transition plan and System Engineering approach (*see earlier NDIA presentation*)

To the Heart – Gems of Wisdom (cont.)

- Multiple sources need to be used simultaneously in analysis to understand the CCIs (e.g. 800-53, CNSSI.11, Aerospace document, Program guidance)
- Get approvers/assessors in-line and participating early
  - Capture assessor/customer/command decisions toward interpretation and implementation] somewhere accessible by all stakeholders – similar to a design decision database
- Ensure Government Customer and Developer are collaborating early and frequently, constantly if possible

To the Heart – Gems of Wisdom (cont.)

- It's a system (holistic) challenge – it is critical that this is not made a 'cyber security' challenge/responsibility – it has to be baked-in not added on (engineered in) for Program success
  - have to back RMF into more than the technology during analysis and implementation
  - Involve all disciplines / functional areas – anyone with skin in the game (for each group of CCIs
- Economic 'reality' is cost and schedule constraining, so
  - Approach it incrementally :
    - Option 1 – by phase (analysis, assessment, implementation)
    - Option 2 – by priority/criticality – a group of CCIs at a time

To the Heart – Gems of Wisdom (cont.)

- Implementation Gems
  - Define an analysis methodology with ground rules for
    - artifacts that provide evidence toward the compliance assessment (e.g. ATO) for non-technical CCIs
    - Walk a day-in-the-life of the assessment, with all key stakeholders, so everyone knows how to support it, where to store evidence, etc
  - Working with those who will evaluate compliance (Assessors) – define how evidence of compliance with CCIs will be documented, especially for non-technical CCIs
    - technical CCIs generally beget system requirements and subsequently implemented in technologic components/functionality that is tested and verified

Credit where credit is due

- C2BMC Program
- MDA / BC Organization
- Lockheed Martin
  - C4USS – C4ISR & Undersea Systems
  - Rotary and Mission Systems (RMS)
- Boeing team mates
- General Dynamic team mates
- Northrop Grumman team mates
- Raytheon team mates

Questions and/or Comments?