RMF for leadership

Kurt Danis, CISSP-ISSEP
ISSA Colorado Springs
15 October 2016
## History

<table>
<thead>
<tr>
<th>Rainbow Series</th>
<th>DITSCAP</th>
<th>DIACAP</th>
<th>RMF</th>
</tr>
</thead>
</table>
RMF activities based on many objectives
C&A Transformation Goals

1. Define a *common set of trust (impact) levels* and adopt and apply them across the Intelligence Community (IC) and DoD. Organizations will no longer use different levels with different names based on different criteria.

2. Adopt *reciprocity* as the norm, enabling organizations to accept the approvals by others without retesting or reviewing.

3. Define, document, and adopt *common security controls*, using NIST Special Publication (SP) 800-53 as a baseline.

4. Adopt a *common lexicon*, using CNSS Instruction 4009 as a baseline thereby providing DoD and IC a common language and common understanding.

5. Institute a *senior risk executive function*, which bases decisions on an “enterprise” view of risk considering all factors, including mission, IT, budget, and security.

6. Incorporate information assurance (IA) into *Enterprise Architectures* and deliver IA as *common enterprise services* across the IC and DoD.

7. Enable a *common process* that incorporates security within the “lifecycle” processes and eliminate security-specific processes. The common process will be adaptable to various development environments.
Illustrates complexity and the breadth of the role of the ISSE in all of the processes as a starting point and not a final solution. The final process should be tailored to the requirements of each agency.

<table>
<thead>
<tr>
<th>Standard</th>
<th>Description</th>
<th>Concept</th>
<th>Development</th>
<th>Production</th>
<th>Utilization</th>
<th>Support</th>
<th>Retirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>NIST SP 800-37</td>
<td>RMF Categorize</td>
<td>System Requirements Definition Process (SR); Architecture Definition Process (AR); Design Definition Process (DE)</td>
<td>System Analysis Process (SA)</td>
<td>Implementation Process (IP); and Integration Process (IN)</td>
<td>Verification Process (VE); Transition Process (TR); and Validation Process (VA)</td>
<td>Support</td>
<td>Retirement</td>
</tr>
<tr>
<td>NIST SP 800-39</td>
<td>Risk Management</td>
<td></td>
<td></td>
<td></td>
<td>Respond and Monitor Risk</td>
<td>Determine Acceptance of Known Risk</td>
<td>Continue to Frame, Assess, Respond and Monitor</td>
</tr>
<tr>
<td>NIST SP 800-137</td>
<td>Continuous Monitoring</td>
<td>Define and Establish ConMon Strategy</td>
<td>Implement ConMon Strategy</td>
<td></td>
<td></td>
<td>Analyze and Report, Respond, and Update</td>
<td></td>
</tr>
<tr>
<td>DoDi 8510.01</td>
<td>RMF for DoD IT</td>
<td>Program Acquisition Strategy</td>
<td>Specify System Security Baselines</td>
<td>1) Translate Security Controls to Design</td>
<td>Developmental Test and Evaluation</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DoDi 5000.2-R</td>
<td>MDAPS &amp; MAIS</td>
<td>Requirements Analysis</td>
<td>Functional Analysis &amp; Allocation</td>
<td>Synthesis</td>
<td>Verification</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IATF chapter 3</td>
<td>ISSE process</td>
<td>Discover Info Protection Needs</td>
<td>Define System Security Requirements</td>
<td>Functional Verification</td>
<td>System Analysis</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IEEE 1220-1198</td>
<td>Systems Engineering Process</td>
<td>Requirements Analysis</td>
<td>Design System Security Architecture</td>
<td>Functional Verification</td>
<td>Verification</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
RMF stakeholders

STRATEGIC RISK

- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness

TIER 1
ORGANIZATION

DoD CIO/SISO (RMF TAG & KS),
DoD ISRM (DSAWG)

TIER 2
MISSION / BUSINESS PROCESSES

WMA, BMA, EIEMA, DIMA PAOs,
DoD COMPONENT CIO/SISO

TIER 3
IS/PIT SYSTEMS

AUTHORIZING OFFICIAL (AO), SYSTEM CYBERSECURITY PROGRAM

TACTICAL RISK

- Inter-Tier and Intra-Tier Communications
- Feedback Loop for Continuous Improvement

WMA – Warfighting Mission Area
BMA – Business Mission Area
EIEMA – Enterprise Information Environment Mission Area
DIMA – DoD portion of the Intelligence Mission Area
RMF Step 1, Categorize the System

RMF swim lanes

PROCESS FOR SYSTEMS ONLY

Identify the DoD IT Type

Assess & Authorize

DoD Information Technology

Information Systems

PIT

IT Services

IT Products

Major Applications

Enclaves

PIT Systems

Internal

External

Software

Hardware

Applications

Determine potential C-1A Impact values

Consider additional categorization factors (Para. 2.1.2, CNSSI 1253)
Risk table as a function of **Likelihood vs. Impact**

### Likelihood
- **Very Low**
- **Low**
- **Moderate**
- **High**
- **Very High**

### Impact
- **Very High**
- **High**
- **Moderate**
- **Low**
- **Very Low**

### Likelihood Determination

### Combination of Likelihood and Impact

### 5x5 Threat & Vulnerability

### 5x5 Likelihood & Impact
Risk Analysis Model – Tying it Together

1. What is the LIKELIHOOD an event will occur?
- a: Remote
- b: Unlikely
- c: Likely
- d: Highly Likely
- e: Near Certainty

2. What is the IMPACT if the event occurs?
- a: Minimal or no impact
- b: Acceptable with some reduction in margin
- c: Acceptable with significant reduction in margin
- d: Acceptable; no remaining margin
- e: Unacceptable

- And/or Schedule
- And/or Cost
- And/or Impact on Other teams

- Minimal or no impact
- Additional resources required; able to meet need dates
- Minor slip in key milestones; not able to meet all need dates
- Major slip in key milestone or critical path impacted
- Can’t achieve key team or major milestone

- Low
- Moderate impact
- Major impact
- Unacceptable

- HIGH – Unacceptable. Major disruption likely; different approach required; priority management attention required.
- MODERATE – Some disruption; different approach may be required; additional management attention may be needed.
- LOW – Minimum impact; minimum oversight needed to ensure risk remains low.
Leadership Responses

- Risk Acceptance
- Risk Avoidance
- Risk Mitigation
- Risk Sharing
- Risk Transfer

"Take calculated risks. That is quite different from being rash." -- General George S. Patton (1885-1945)
Alignment of RMF and DoD Acquisition System Activities

Joint Capabilities Integration and Development System

- Initial Capabilities Document (ICD)
- Capability Development Document (CDD)
- Capability Production Document (CPD)

RMF Step 1 - Categorize system
- Program Acquisition IA Strategy

RMF Step 2 - Select security controls
- Specify system security baselines in JCIDS D

RMF Step 3 - Implement security controls
- ISSE/SSE translates security controls to design requirements and integrates into system specifications
- System security specifications in RFP
- Coordinate TEMP and Security Assessment Plan
- Approve system security design at review points

RMF Step 4 - Assess security controls (issue IATTs as needed)
- Developmental Test & Evaluation (DT&E)

RMF Step 5 - Authorize system (issue ATO)
- Operational Test & Evaluation (OT&E)

RMF Step 6 - Monitor security controls

DoDI 8510.01 Figure 4. RMF and the Defense Acquisition Management System
Agile Contracts for Sustainment

Addresses the “Past” Target
Acquisition perceptions:
• Cyber is a static threat
• Threat not agile
• Threat not progressive
• Large monolithic contracts
• Contract mods only with great effort and more $$

Addresses the “Present” Target
Policy & Tools defend target
• DIACAP process were 1-dimensional (Vuln.)
• RMF approach addresses Threat-Vuln. Pair

Addresses the “Future” Target
Threat Coordination & Automation
• Agile, emerging, and... evasive well-designed threats against
• Leverages standard threat sharing protocols & mechanisms
• Requires Continuous Monitoring
RMF security control sets

800-53 (966) & Overlays

~1,000Ctrls & Enhancements from baselines

Tailored 1253

Mgt

Ops

Tech

~400ctrls & enhancements

Mgt or gov’t oversight controls

Gov’t Ops

SysDev Ops

SysDev controls identified for RFP

System Owner Controls

SysDev Controls within Budget & on contract

POA&M

1067 SCF actions

Recursive POA&M process (annually)

Tailored 1253

Mgt

Ops

Tech

 SysDev Ops

 SysDev controls identified for RFP

 System Owner Controls

 SysDev Controls within Budget & on contract

 POA&M

 1067 SCF actions

 Recursive POA&M process (annually)
Leading & Lagging Indicators

Balanced scorecard

- Internal Processes
- Finance
- Customer
- Learning & Growth
**Engineering Requirements**

**DIACAP IA controls are prescriptive:**
- 110 IA controls for MAC II, Classified – no exceptions
- Some controls could be N/A if Threat-Vulnerability pair = 0 (example space vehicle in a zero oxygen environment \( \Rightarrow \) PEFS-1 is N/A)

**RMF Security Controls are based on Requirements:**
- Common Security Control numbers based on C-I-A categorization
- System Specific Controls for systems supporting certain Mission Areas (MAs)
- Overlays: Are based on special capabilities (space, CDS, IC, etc.)
- Tailoring: Based on the system engineering requirements, allowing security controls to be “tailored-out” or “tailored-in”
Multi-dimensional

DIACAP: 1-dimensional, and RMF: 4-dimensional

DIACAP Compliance Check
Are you compliant with these controls?

- Yes
- No

- No additional analysis required
- DAA makes accreditation decision based on compliance / non-compliance
- Prioritization of fixes based on raw severity categories (CAT)
- Does not incorporate critical thinking and/or DAA’s risk tolerance

Risk Management Framework
Are you compliant with these controls?

- Yes
- No

- What is the mission / architecture risk?
  - Vulnerability
  - Threat
  - Likelihood
  - Impact

- What is the Authorizing Official’s risk tolerance?
  - Community risk tolerance—DAO, SCA
  - Mission risk tolerance—Information Owner

\[ \text{Residual Risk} + \text{Risk Tolerance} = \text{Authorization Decision} \]
Backup Slides
Top 20 Controls

- We have high regard for NIST's work. However, the problem for organizations trying to follow NIST's guidelines amid today's increasing cyberthreats is akin to confronting a raging new pandemic with an encyclopedic field guide to holistic health care.

John Gilligan
Team Lead

Source: Consensus Audit Guidelines (Top 20 security controls).pptx
Cybersecurity Guidebook for PMs

- A practical reference for PMs to integrate cybersecurity throughout the acquisition lifecycle

- Authoring team chaired by USD(AT&L) and DoD CIO
  - Participants: DOT&E, Joint Staff, Army, Navy, Marine Corps, Air Force, USCYBERCOM, DISA, NSA and DIA

- Published in conjunction with DoDI 8500.01 and DoDI 8510.01
Sources for DoD Policy

IA Support Environment
http://iase.disa.mil/index2.html

Knowledge Service
https://diacap.iaportal.navy.mil/login.htm

DoD Issuances Website

CNSS Policies
http://www.cnss.gov/policies.html

NIST Publications
http://csrc.nist.gov/publications/PubsSPs.html

IATAC DoD IA Policy Chart
http://iac.dtic.mil/csiac/ia_policychart.html