CONCEPT: "RMF for leadership" course

Typically, Risk Management Framework (RMF) courses focus on the terminology, processes, and roles and responsibilities; in other words, the art of producing an RMF package. This paper suggests an RMF short-class or course should be available for leaders on the periphery of the package making process; specifically, a course that explores the "so-what" factors for DoD leadership not in the midst of the RMF pipeline.[1] This leadership course would provide characterizations, principles, and lessons-learned that resulted in what RMF is today.

Rainbow Series	DITSCAP	DIACAP	RMF
Computer Security	Network Security	Netcentric Security	Mission Assurance

Leadership should know RMF is a collage of activities that embody many objectives of the past, and address several new tenets never before handled in a systematic way.

RMF is all the above (Rainbow series, DITSCAP, DIACAP) plus… RMF:

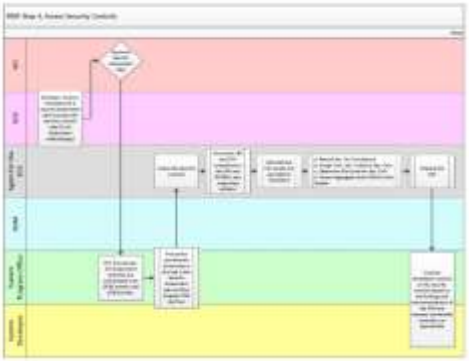
- Ties the Strategic, Operational, and Tactical stakeholders together[2]
- Manages a mission assurance (MA) balance with the **security posture** requirements
- Is a means to align the DoD, IC, and civil agency methodologies (**as a result RMF is standardized, and uses a common taxonomy**)
- Quantifies and documents system threat sources (e.g. supply chain risk management, espionage, insider threat, threats against critical technology/critical information, etc.)
- Links and communicates **risk to the stakeholders** (i.e. mission owners, mission supporters, system developers, system/asset owners, project managers, other Organizations, the Nation, etc.) ➔ **RMF not a vulnerability checklist**
- Is multi-dimensional. Where DIACAP focused only on vulnerabilities, RMF is a deliberate means to assess the threat, vulnerability, likelihood (or probability), impact (or consequence)
- Is aligned to the newest domain…..Land, Sea, Air, Space, and Cyber --- clearly, the reason why DoD changed the name from IA to "Cybersecurity"
- Adopts Reciprocity (AO only needs to assess unique pieces)
- Maps directly to the Defense Acquisition Life Cycle
- Includes a definitive process for "assessing" PIT, Applications, SW, HW, and Services

[1] Perhaps, the best RMF leadership resource available today is the **DoD Authorizing Official** course on the IASE website.
[2] DoD CIO, Risk Executive Function, RMF TAG, Mission area owners, Acquisition, DISA, Component CIOs,…

CONCEPT PAPER

An "RMF for leadership" course would highlight tangible take-aways for the executive or commander who owns the mission. Ideas for consideration include:

- An RMF leadership course would articulate the decision maker's role for a Security Authorization Package. For example, a swim-lane chart would show each of the Primary Roles ("swim lanes" as rows) in support of each of the RMF steps (columns). While the chart may be constructed of "sausage making" processes. An RMF leadership course would provide decision-maker principles; not dive into the details.



- An RMF leadership course would emphasize the factors of risk include more than the Threat-Vulnerability pair; Probability/Likelihood, and Impact/Consequence are also significant factors.[3] Impact can encompass things like asset value and mission criticality. Older doctrines may use different terms. For example, the US Army had an expression called CVRT that measured criticality, vulnerability, recuperability, and threat.[4] In general, [cybersecurity] "…is a multidisciplinary approach to managing risk; a principle concern of executives."[5]

- An RMF leadership course would associate the "vulnerability/threat pair" (NIST SP 800-30)[6] with the Probability and Impact dimensions. Then, illustrate how these dimensions are used in a risk matrix; also known as a "Heat Map". Parallel: RMF leadership would recall an acquisition matrix known as the "Risk Analysis Model".[7]

- An RMF leadership course would propose the concept that the decision maker ought to have a clear threshold in mind. A risk threshold must be pre-meditated. A threshold would set a definitive tone in case a persuasive argument led a decision-maker away from common-sense. In this way, a system would absolutely NOT operate unless certain vulnerabilities or threats were resolved/mitigated to an acceptable level. For example, the hull of a combat ship with holes would never go underway; likewise, an aircraft with contaminated fuel would not fly during peace-time; etc.

"Take calculated risks. That is quite different from being rash." -- General George S. Patton (1885-1945)

[3] "If we focused mostly on the threat/vulnerability pairing, we may miss the fact that ultimately the risk is low, because we don't carefully examine the likelihood and impact. Similarly, the likelihood could be high and the impact low, resulting in another possible low risk situation that is acceptable. In contrast, the likelihood could be low but the impact very high, which could result in a risk that is not acceptable." - Randy Gabel, The MITRE Corporation

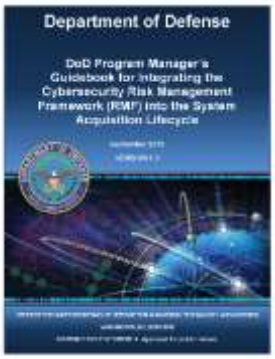
[4] Chapter 13 "Air and Missile Defense", Field Manual 100-16, Army Operational Support, Dept of the Army, 31May1995

[5] Cybersecurity for Executives – A Practical Guide, Gregory Touhill, Brig Gen (ret), CISSP, CISM

[6] NIST SP 800-30, Appendix I

[7] Defense Acquisition Guidebook, 16-September-2013, Figure 14.3.1.1.F1. Risk Analysis Model

- **An RMF leadership course would focus on the Authorization Official's decision-making role on handling risk**. Risk responses according to NIST[8] include: Accepting[9], avoiding[10], mitigating, sharing, or transferring risk to organizational operations (i.e., mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation. In addition, another "course of action" would include a time-phased or a situation-dependent combination of risk response measures.



- An RMF leadership course would capture various high-level concepts from the DoD Program Manager's Guidebook for integrating the Cybersecurity RMF into the System Acquisition Lifecycle (30Oct2015).

- An RMF leadership course would identify different production process strategies to handle high volumes of Security Authorization Packages. Strategies might include: (a) Divide and Conquer, (b) fast-track packages with repetitive continuous improvement cycles, and (c) spreading the RMF load across the workforce (reference: DoDI 8510.01).

- RMF leadership would learn about two or three contract strategies. For example:
  - Pitfalls of a contract clause that issues a blanket statement to just "do RMF";
  - Pitfalls of inflexible contracts (i.e. RMF today, but impossible for tomorrow's new method);
  - Advantages of a Contract Data Requirements List (CDRL) using an IDIQ strategy --- permits decision maker to dynamically focus and shift to a different and more appropriate set of critical RMF security controls where needed. Avoids being locked into a set of shotgun prescriptive baseline security controls.

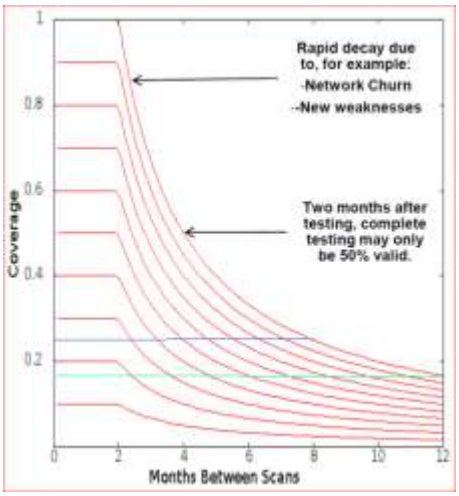
- RMF leadership would guide or shape a healthy pipeline process. Often times, players in the RMF pipeline would like to "keep their problems to themselves". In fact, evidence from past security authorization packages suggest there has been a reluctance to be forthright. Obscuring, ignoring non-compliant controls, and omitting weaknesses would veil the true expense to get well. Instead, leadership would promote a transparent attitude – so Time, Effort, and Money (resources) would be responsibly estimated and communicated in the POAM. In this manner, RMF leadership would have a fighting chance to make decisions.

> "The first step in the risk management process is to acknowledge the reality of risk. Denial is a common tactic that substitutes deliberate ignorance for thoughtful planning." -- Charles Tremper

[8] NIST SP 800-30, Rev. 1; Guide for Conducting Risk Assessments
[9] a system security project implemented piece-meal using a time-phased plan would be a form of risk acceptance plus mitigation measures over a scheduled time frame.
[10] Limiting the capability, limiting the time of operation would constitute forms of risk avoidance.

- Knowing which gage to watch before catastrophe strikes would be key to success. An RMF leadership course would reflect on the Balanced Scorecard (Kaplan & Norton) concept with **leading and lagging indicators**. Leadership would recognize continuous monitoring would be essential for critical controls much like a train engineer's practice to monitor certain critical locomotive pressure gages.

- RMF leadership would discover every "compliant system" has a half-life. That is to say, compliance plummets over time because of emerging vulnerabilities, followed by benchmarks documented in STIG's and new IAVM's. As a result, compliance is a moving target. What was compliant yesterday, would be non-compliant tomorrow. Graph shows Coverage verses Time curves are not static, because vulnerabilities are not static. Instead, they "grow" like tree rings – each one requires more and more compliance coverage. This phenomenon was inherent to methodologies before RMF. The cybersecurity community realized the so-called "fire and forget" practice had to stop. **Without an ongoing effort to mitigate vulnerabilities, compliance decreases rapidly over time**.[11]



- Finally, an RMF leadership course would address some common misunderstandings. For example, **continuous monitoring does not mean constant real-time monitoring**. NIST SP 800-137 renders "continuous" monitoring more as a periodic process where "…security controls and organizational risks would be assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information."

2016.10.16 19:08:03 -06'00'

Kurt D. Danis, CISSP-ISSEP
ISSA Colorado Springs
16 October 2016

[11] "Effective Measures for Continuous Monitoring" presentation by Dr. George Moore, Department of State, 7th Annual IT Security Automation Conference, October 31 - November 2, 2011