# RMF Lessons Learned Discussion

## Lessons Learned

Take the time to develop a Transition Plan

It helps to give management a good picture of what an RMF transition requires in the way of resources, inputs, and schedule – essential to properly funding the effort and acts as a roadmap

- Clearly define what intend to accomplish
- Identify threats to mitigating communications breakdowns.
- Train upper management to be successful.
- Work RMF as a progressive endeavor
  - Move from Point A to Point B to Point C.
- Recognize that implementing RFM is a long-term and on-going activity.

Define terms and application of them

- 
- Organization – Key families where this is critical include CM, IR…
  - Defining the applicable organization for CCIs helps in identifying expectations (i.e., who is doing what?)
- Stakeholder
- Controls
- Requirements (specifications)
- "Essential missions" vs. " essential business functions"
  - Need to differentiate between "business functions" and "essential mission" wording in CCIs – the terms could mean one of two things:

- "Business function" – used by non-DoD orgs; " Essential Mission" - used by DoD orgs
- "Business function" – IT support function like acquisition, training, support; "Essential Mission" – IT systems directly supporting a DoD mission

Define steps to implement.

- Build terminology and process steps into System Security Plan
- Define CCI validation procedures.
- Identify risk "appetite" of stakeholders (i.e., what organization is willing to put down, what the organization is willing to take, and how much the organization can afford.)

Categorize system (SP 800-37, Step 1)

- Identify/Define data (e.g., Privacy data, classified data, FOUO data, security data, mission data, etc.) – required by several families
- Identify/define essential mission/business functions – required by CP family
- Identify data owners, consumers and customers.

Select Controls (SP 800-37, Step 2)

- Focus on the areas that have the highest Return on Investment (ROI)

Strive to understand the CCIs – check out available resources for help in understanding exactly what NIST is asking for (e.g.,

SP800-53 Supplemental Guidance and the Aerospace RMF Guidance)

Document SP 800-53 assignments/selections as a document or document family

- Requires collaboration from all stakeholders to include PM, Ops, Developer
- Develop body of assignments/selections as a working group and document in a single document
- Consider defining so as to allow for the "re-use" of assignments/selection decisions across a large enterprise that may have numerous enclaves
- Can be used as an artifact to support Control/CCI validation
- Assignments/selections transcend all organizational levels
- Understand the difference between control assignments, selections, and CCIs. For example:
  - "Do xxx IAW" [Selection options]
  - "Do xxx IAW" [Assignment free text]
  - CCIs can be either technical or non-technical and often require a selection or an assignment as an input
- DoD Specific Assignment Values (DSPAVs) provide the DoD determination of selected CCI assignments/selections
  - "Automatically Compliant" – If a control/CCI requires the defining (assignment) of a value/role, often the DoD has provided those values or identified the roles so it is already compliant. Usually the next CCI within that control talks about validating of that value or role so that would be where we check to make sure the value has been enforced or that the role does what

they are suppose to do (many are something like the ISSO/ISSM gets automated alerts…. [DISA]

- All assignments/selections should be incorporated into design/implementation/verification documentation as applicable
- Assignments/selections should be "SFC"s – Sufficient-Feasible - Clear
- Include gap analysis (baseline system, measure current performance, compare to baseline requirements, identify gaps)
    - Assess CCIs to identify the delta between a DIACAP and an RMF implementation:
        - What do I have?
        - What do I need to get to?

Develop analysis methodology for identifying artifacts and stakeholders

- Whenever analyzing CCIs, always review them in context with other family-related CCIs – don't just review the technical CCIs without the context of the non-technical CCIs
- For artifact identification, obtain a list of artifacts used to support previous accreditations /authorizations and modify it as required – this will minimize the creation of redundant and differently named artifacts

Use a phased approach to analyzing Controls/CCIs based on critical functionality - double-edged sword as it keeps you from analyzing the CCIs as a group…

Identifying CCI “dependencies” is very helpful in pointing both the development team as well as the sustainment teams to assignment/selection decisions that relate to a given CCI.

Do key-word searches to identify all instances of a given function such as alerting,, notifying, and monitoring – this provides a clear picture of what is being asked and what relates to what.

Use some form of “indexing” to support CCI verification and validation efforts
eMASS provides this to a degree – but only at the control level.

Meet regularly as a working group to discuss problem issues and solutions.

Do Control/CCI analysis in small chunks specific to a given control – provides context and helps the group to focus on the subject.

Play close attention to the verbs in the CCIs

- Define
  - To explain the meaning of a word or phrase, etc.
  - To show or describe someone or something clearly and completely
- Identify – identify those elements that meet the definition
- Implement
- Enforce

Identify what has already been implement by reviewing current system specifications and doing a “reverse mapping”

- Traces verification of existing specifications to minimize redundant implementation analysis

RMF is not easy.

- Have to sell" to management
- Requires broad planning and collaboration
- Metrics help scope "bite-sized" tasks

Security serves to support the mission not the other way around. However…Take security seriously. Story of the USS Indianapolis in World War 2 (http://www.ussindianapolis.org/story.htm).

- Heavy Cruiser with crew of about 1,200 that delivered the first atomic bomb to Tinian.
- After delivery, ordered by naval authorities at Guam to sail to support operations near Philippines.
- Sailed in hostile area without destroyer escort (security) and was subsequently torpedoed and sunk.
- No-one was aware of the loss of the ship (capital asset) for four days until a bomber on an anti-sub mission noticed "many men in the water."
- Although ~900 of crew made it into the water, only 315 were successfully rescued because of shark attacks.
- Ship's Captain was Court Martialed for "hazarding" his ship. No record of repercussions to Guam "naval authorities" who issued the orders.
- Post evaluation uncovered fact that US intelligence knew of hostile Japanese submarines were operating in the path where the Indianapolis sailed, but this was not conveyed.

**Questions**

Best practices for instantiating non-technical CCIs?

Best practices for integrating STIGS into RMF'd system?

- Most STIGs now include CCIs – what is the best way to manage (document/implement/verify) them?

Best practices for addressing CCI-related functionality within software?

- SC-24, CCI -001190: The information system fails to an organization-defined known state for organization-defined types of failures

Has anyone used the NIST Cybersecurity Framework?

How do others handle the requirement to document "XYZ" in the SSP? (Since e-MASS has largely replaced the SSP)

**Resources/References**

- RMF Overvist from NIST
  - http://csrc.nist.gov/groups/SMA/fisma/framework.html
- SP 800-53 Supplemental Guidance
- RMF Knowledge Service
  - Primary DoD source of support for implementing RNF
  - Requires CAC
  - Updates DoD guidance for CCIs

- Aerospace RMF Guidance – available to government and DoD contractors
- Customer “plans” identifying the required assignments and selections
- STIG Viewer (helps to understand technical CCI content)
- DoD/NIST guidance called out in RMF KS implementation and validation guidance
- Strategic Threat Assessment Report (STAR) provides a program level threat assessment for major systems