Financial Audit and Cyber Security: FM Overlay and RMF

Amira Tann, Director IT Analysis & Internal Controls
DON CIO

Danny Chae, IT Audit Internal Review Lead
DASN FMP

23 Feb 2017
Overlap Between Cybersecurity and Financial Audit

Transition to RMF, apply FM Overlay (critical security controls for financial audit), manage and implement controls ONCE to satisfy cybersecurity and financial audit requirements.
## Timeline of Events: Years in the Making

<table>
<thead>
<tr>
<th>Year</th>
<th>Joint Memorandum</th>
</tr>
</thead>
<tbody>
<tr>
<td>2012</td>
<td>Joint Memorandum</td>
</tr>
<tr>
<td></td>
<td>• Assessment of Information Technology Systems That Enable and Sustain Audit Readiness (Q4 2012)</td>
</tr>
<tr>
<td>2013</td>
<td>Joint Memorandum</td>
</tr>
<tr>
<td></td>
<td>• Developing More Stringent Security Control Requirements for Financially Relevant Systems to Support Audit Readiness (Q1 2014)</td>
</tr>
<tr>
<td>2014</td>
<td>Joint Memorandum</td>
</tr>
<tr>
<td></td>
<td>• Information Technology Controls Self-Assessment of Financially Relevant Information Systems (Q3 2014)</td>
</tr>
<tr>
<td>2015</td>
<td>Joint Memorandum</td>
</tr>
<tr>
<td></td>
<td>• Auditability of Financial Information Technology Systems and Transition to Risk Management Framework (Q3 2015)</td>
</tr>
<tr>
<td></td>
<td>• Audit Readiness and Risk Management Framework Implementation, (Q4 2015)</td>
</tr>
<tr>
<td></td>
<td>IT Control Standards</td>
</tr>
<tr>
<td></td>
<td>• Established enterprise level IT standards that meet audit readiness requirements</td>
</tr>
<tr>
<td>2016/17</td>
<td>Joint Memorandum</td>
</tr>
<tr>
<td></td>
<td>• Coordination Between Department of the Navy Risk Management Framework Transition and Financial Statement Audit Requirements (17 Jan 2017)</td>
</tr>
</tbody>
</table>

### Collaboration/Outreach

- **2012**: Created FM validator team to support FM overlay process
- **2016/17**: First system to apply FM overlay with RMF transition (SPS-NAVSUP Dec 2016)
# DON Methodology for Integration of RMF and FM Overlay

**STEP 1: CATEGORIZE Systems**
- Identify FM System Confidentiality Integrity Availability (C-I-A)
- Categorize system to CNSSI 1253 and NIST 800-53 rev4

**STEP 2: SELECT Security Controls**
- Select baseline control set and applicable overlays (e.g. FM for audit relevant systems)

**STEP 3: IMPLEMENT Security Controls**
- Implement tailored control sets
- Prepare the POAM with Navy architecture

**STEP 4: ASSESS Security Controls**
- Assess tailored control set
- SCA writes Security Assessment Report
- Remediate preliminary findings

**STEP 5: AUTHORIZE Information Systems**
- Program assembles RMF Package
- **Program / Echelon II submit RMF package for FM Endorsement memo**
- Authorizing Official (AO) Authorizes System

**STEP 6: MONITOR Security Controls**
- Determine impact of changes to system and environment
- & assess security controls annually
- AO reviews security status
- System decommissioning

**RMF Process**
- FM Validator Team initiates kick off with the Information System Owner (ISO) and provides roadmap of the FM Overlay
- FM Validator Team works with the ISO to ensure applicable FM controls are selected and tailored as required
- FM Validator Team develops the assessment plan and is available for consult to the ISO for FM controls implementation
- FM Validator Team performs the FM controls assessment
- FM Validator Team reviews and provides the endorsement memo
- FM Validator Team monitors FM systems utilizing a FM continuous monitoring strategy
FM Overlay Key Takeaways

- FM overlay IT controls are: Access Controls (AC), Audit and Accountability (AU), Configuration Management (CM), Identification and Authentication (IA) controls that map to FISCAM objectives as well as all Policy and Procedure (-1) controls.

- FM overlay provides new validation procedures that contain FISCAM style of validation.

- Team led by ASN (FM&C) FMP with DON CIO collaboration.

- RMF Steps 1-3 – FMP team acts as support/consulting team.
  - Artifacts that are responsibility of SCA, FMP provides input on FM overlay controls.

- RMF Step 4 - FM Validators are a separate team from FMP who validate FM overlay controls. SCA uses results of the team’s validations to eliminate redundancy.

- RMF Step 5 – FMP to provide endorsement memo to Navy Approving Official (NAO) prior to final authorization (ATO).

Intent is to leverage RMF to influence validation of critical controls without delaying ATO.
FM Validators – MOU between DASN (FMP) and SCA

DASN (FMP)

• FM validators will be Navy Qualified Validators (NQV)
• The FM Validator will provide an FM Endorsement Memorandum (Appendix A) that summarizes compliance with FM Overlay requirements.
• The FM Validator shall be responsible for assessing and recording FM Overlay controls as Compliant Official (CO) or Non-Compliant Official (NCO) at the conclusion of testing within eMASS.
• The FM Validator shall provide testing results to the system assigned SCA Validator for entry into Security Assessment Report (SAR).

SCA

• The Navy SCA shall consider the information contained in the FM Endorsement Memo when assessing the final risk level for an audit-relevant system to which the FM Overlay has been applied.
• The Navy SCA shall coordinate with FMP to answer questions regarding FM Overlay requirements or the risk levels recommended by the FM Validator for NCO FM Overlay security controls.
Joint Memorandum on the Risk Management Framework and Financial Statement Audit Requirements

The Undersecretary of the Navy and the Vice Chief of Naval Operations signed a Joint Memorandum dated 17 JAN 2017 on the coordination of cybersecurity and financial statement audit requirements.

The Memorandum directs that:

Owners of current systems that are relevant to financial audit implement the FM Overlay during transition to the Risk Management Framework (RMF).

Owners of new DON systems that are relevant to financial statement audit apply the DON Enterprise IT Controls Standards and the FM Overlay during controls implementation during the RMF system authorization process.

Financial system resource sponsors appropriately resource system efforts to implement internal controls that meet the requirements of a financial statement audit.

Security controls in the FM Overlay are intended specifically to satisfy audit requirements and will not necessarily impact the decision to issue an Authorization to Operate (ATO).
SPS-NAVSUP FM Overlay Lessons Learned

SPS Perspective
- Know the RMF Process Guide (RPG)
  - New version to be published will include FM Validator and SCA MOU as an appendix
- Know the eMASS guide
- Visit DoD Knowledge Service website
- Use NAO templates

FM Validator Perspective
- Management approval and support from the system is key
- Set up a weekly drum-beat with the local validator
  - Close coordination with the local validator is key to ensure successful completion of the assessment
• Leveraged on-site and virtual collaboration sessions
• Set expectations up front based on Joint Memo and MOU
RMF & FM Overlay Lessons Learned

1. Inheritance
2. FM Overlay Control Deviations
3. SCA and FM Validator Roles
A disconnect exists between data centers and system owners regarding inheritance

- System owners assume data centers are responsible for implementing many of the required controls

Inheritance depends on distinguishing between the database, operating system, and application levels

- Controls must be implemented at all 3 levels
- Data centers and system owners must be aware of their responsibilities at each level

Specifically address each party’s responsibilities in the SLA/MOU, supplemented with identification of inheritable security controls, to ensure understanding
Instances exist where the FM overlay requires more (or less) stringent control parameters than those required by NIST or other applicable overlays. Potential mitigations include:

- Implementing the parameter that makes better business sense (and documenting the business case for the decision)

If not all of the RMF or FM required controls are implemented:

- Document that a valid business case exists (i.e. time, financial, or resource constraints) for non-implementation and/or compensating controls are in place
- The system owner, data center, and Navy enterprise must be willing to accept this risk
SCA and FM Validator Roles

Synergies between the SCA and FM validator are essential for establishing a relationship and generating reciprocity:

- FM validator will focus on the four FM overlay control families (AC, AU, CM, IA) and all 18 “dash 1’s”
- SCA’s primary focus will be on the 14 remaining non-FM overlay control families and any controls that are not addressed by the FM overlay control families (e.g., AC-21, AC-22, AC-23)
- Collaboration between the parties throughout the process is vital

Proper screenshots and documentation should be created and stored for artifacts:

- Even though the SCA and FM validator are simultaneously involved at Step 4 of RMF, the process should continue to run efficiently if documentation is provided
FM Overlay - Feedback

- eMASS does not have appropriate functionality with regard to the RMF transition and inclusion of the FM overlay.
- Initiated RMF for multiple systems, but FM validator has not been identified and/or communicated.
- High auditor turnover combined with inadequate knowledge sharing creates additional work for data centers/system owners.
- Auditors are issuing NFRs that are out of the data center/system owner’s scope (i.e. not in their system boundary).
- More clarity is needed surrounding the overall audit process and specific roles/responsibilities.
- The CYBERSAFE process will create a bottleneck as a grade is required in order to move past Step 1 of RMF and certification is required to move past Step 5 of RMF.
- Having an RMF process overview heightened our mitigation strategy around cyber risks.
- Walk-through of System Security Plan (SSP) implementation statements was helpful.
- Information regarding data center system boundaries and inheritance is very useful.