DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

FMP Financial Policy & Systems

Synergistic Efforts Between Financial Audit and Cyber Security

Amira Tann, DON CIO – IT Audit Readiness Lead
Danny Chae, ASM FMC FMP – IT Controls Lead

June 2, 2016

Orlando, FL National PDI

Recent Cybersecurity Headlines

Fixing the problem involved installing an available update

THE BALTIMORE SUN

MedStar disputes report it ignored warnings that led to attack

NSA is always looking for interesting ways to gain access, whether it be through an HVAC system – which was the cause of the massive Target breach of 2014

BGR TECH ENTERTAINMENT SOCIAL LIFESTYLE BUSINESS DEALS PODCAST

NSA's chief hacker explains how to keep the NSA out of your business

By Yoni Heisler on Jan 29, 2016 at 11:00 PM

SECURITY

Attackers gained valid user credentials to the systems they were attacking. The breach also consisted of a malware package which installed itself within OPM's network and established a backdoor.

Forbes

JUN 11, 2015 @ 09:12 PM

Federal Union Says OPM Data Breach Hit Every Single Federal Employee

Recent DoD Audit Headlines

RealClear Politics

Senators move to demand DOD audit penalties

155 10

← Back to Videos

By Martin Matishak - 02/04/15 03:16 PM EST

Bernie Sanders: Audit The Department Of Defense, Contractors Wasting Money While Soldiers Are On Food Stamps

Posted on December 29, 2015

USMC Reversal a Hitch in DoD Audit Plans

By Joe Gould and Hope Hodge Seck 5:27 p.m. EDT March 30, 2015

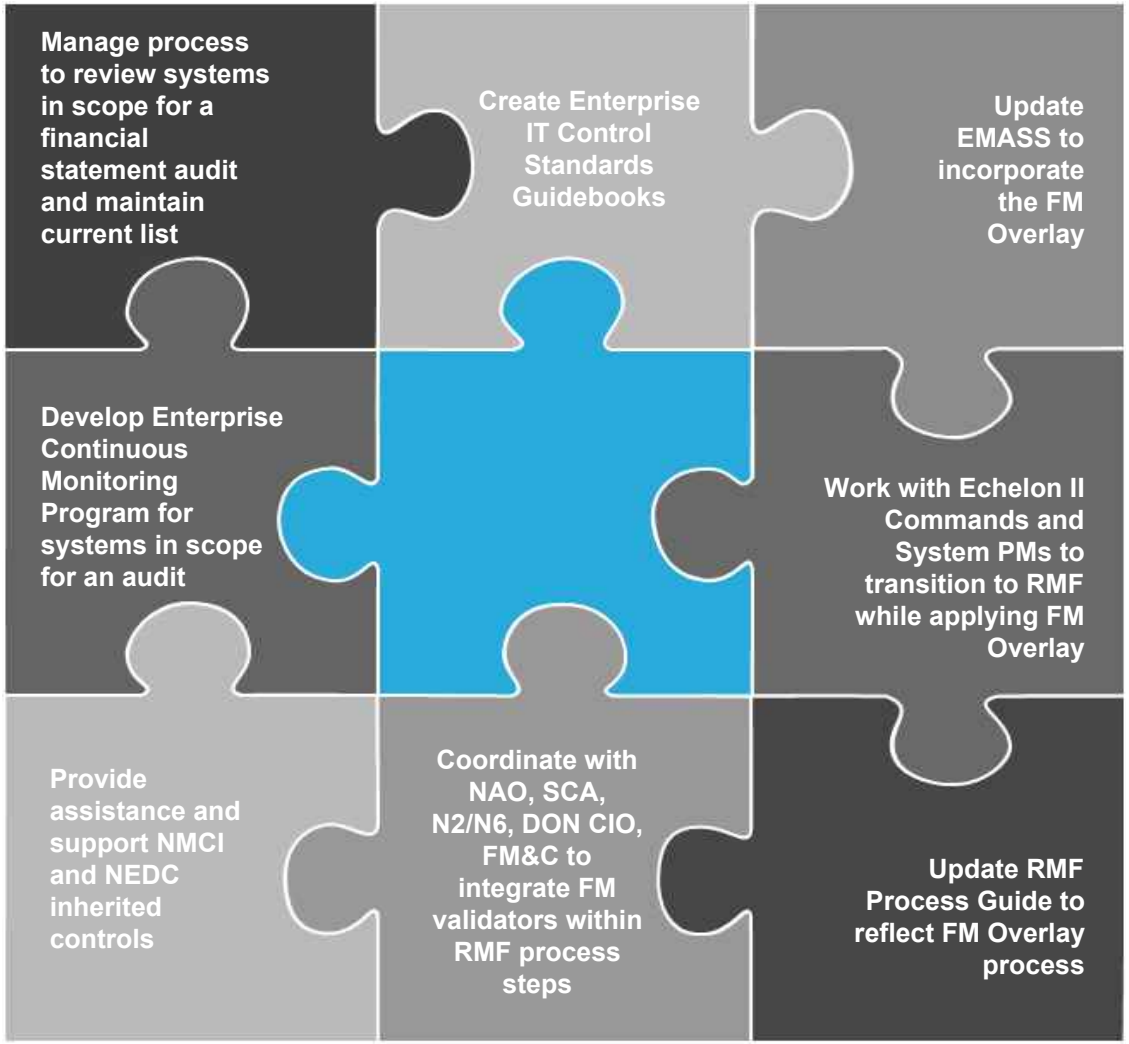
THE BLOG

Uncontrollable — Pentagon and Corporate Contractors Too Big to Audit

03/18/2016 12:27 pm ET | Updated Mar 18, 2016

DON Approach to Merging Audit and Cybersecurity Requirements

ASN FM&C and DON CIO are collaborating and working closely on separate, but related mission objectives to find synergies and gain efficiencies in previously redundant activities



Synchronization of Cyber and Audit Activities

As-Is State
DIACAP & FISCAM

DIACAP
- Technically Focused
- Cyber Security Compliance to obtain Authority to Operate (ATO)
- Management has the option to accept the risk associated with a control failure

FISCAM
- Business Process Driven
- Assessments for DON financial information systems
- Enables auditors to place reliance on the quality of the data within the system
- Relies on NIST SP 800-53 Rev. 4

To-Be State
RMF

- Technically Focused Hybrid Approach
- Streamlining multiple compliance requirements for System Owners
- Standardizing the DON's risk mitigation approach for financially relevant IT systems
- FMO and DON CIO collaboration to issue DON IT Controls Guidance for audit relevant systems
- Leveraging the multi-year FISCAM efforts to synchronize RMF and IT control requirements related to on-going audits

Enterprise IT Control Standards

RMF Joint Memo

Timeline of Events: Years in the Making

2012

Joint Memorandum

- Assessment of Information Technology Systems That Enable and Sustain Audit Readiness (Q4 2012)

2013

Joint Memorandum

- Developing More Stringent Security Control Requirements for Financially Relevant Systems to Support Audit Readiness (Q1 2014)

2014

Joint Memorandum

- Information Technology Controls Self-Assessment of Financially Relevant Information Systems (Q3 2014)

2015

Joint Memorandum

- Auditability of Financial Information Technology Systems and Transition to Risk Management Framework (Q3 2015)
- Audit Readiness and Risk Management Framework Implementation, (Q4 2015)
- Established enterprise level IT standards that meet audit readiness requirements (Pending, at ASN level)

2016

Ideal End State

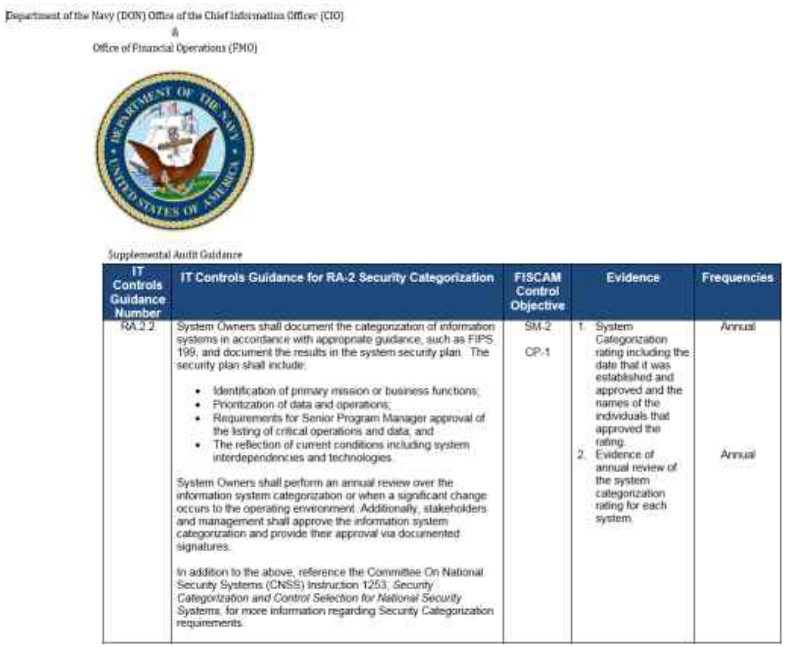
- Leverage current FISCAM assessment teams to begin utilizing IT Control Standards (Q2 2016)
- Provide Formal training/ implementation plan for IT Controls Standards (Q3 2016)
- EMASS system changes to accommodate FM overlay (Q2 2016)
- Separate validator workflow to validate FM overlay
- Validator will come from FMP; Will act similar to “internal IT audit” function
- Automate auditor workflow – ability of auditor to pull necessary documentation themselves w/o need for PBC

Collaboration/ Outreach

- Echelon II CIO’s and System Owners on status and updates on Enterprise IT Controls Standards
- Financial Information Systems Working Group (FISWG) governance forum
- CFO/ CIO Community Touchpoint
- Embedded in FLTCYBERCOM RMF training; provide overview on Enterprise IT Controls Standards
- RMF TAG
- AFCEA Conference, ASMC PDI

DON Enterprise IT Control Standards Guidebooks

- Eighteen Guidebooks created for each NIST SP 800-53 control family
- Guidance written in holistic manner to relate each NIST control to a FISCAM control objective
- The guidance will become the IT Control Standards that systems in scope for audit are required to follow
- The DON Enterprise IT Controls Guidance will also become the DON FM Overlay for RMF



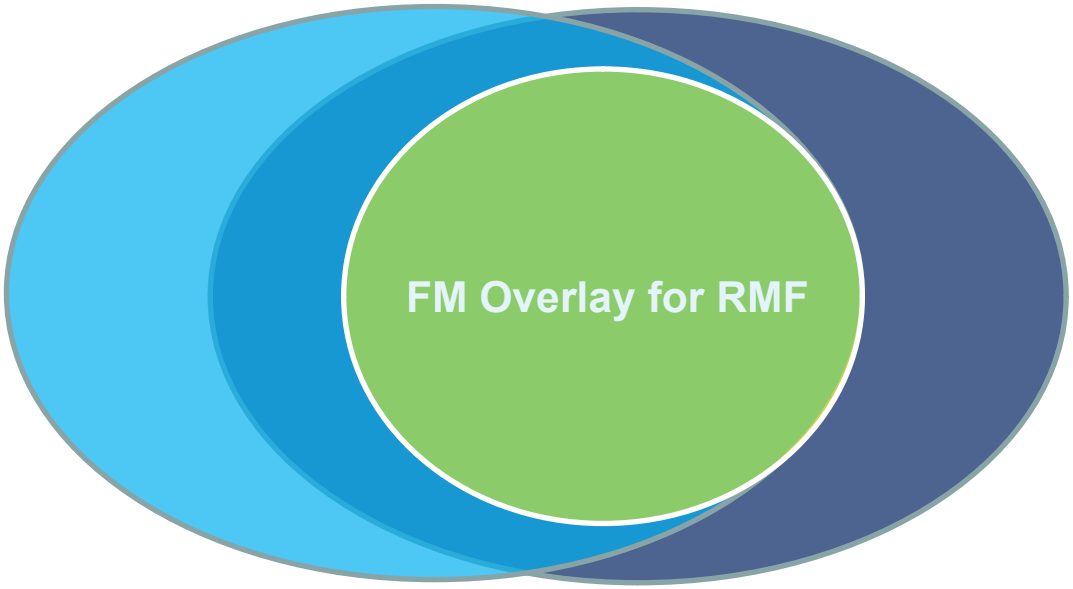
Department of the Navy (DON) Office of the Chief Information Officer (CIO)
&
Office of Financial Operations (FMO)

Supplemental Audit Guidance

IT Controls Guidance Number	IT Controls Guidance for RA-2 Security Categorization	FISCAM Control Objective	Evidence	Frequencies
RA-2.2	System Owners shall document the categorization of information systems in accordance with appropriate guidance, such as FIPS 199, and document the results in the system security plan. The security plan shall include: • Identification of primary mission or business functions; • Prioritization of data and operations; • Requirements for Senior Program Manager approval of the listing of critical operations and data; and • The reflection of current conditions including system interdependencies and technologies. System Owners shall perform an annual review over the information system categorization or when a significant change occurs to the operating environment. Additionally, stakeholders and management shall approve the information system categorization and provide their approval via documented signatures. In addition to the above, reference the Committee On National Security Systems (CNSS) Instruction 1253, *Security Categorization and Control Selection for National Security Systems*, for more information regarding Security Categorization requirements.	SM-2 CP-1	1. System Categorization rating including the date that it was established and approved and the names of the individuals that approved the rating. 2. Evidence of annual review of the system categorization rating for each system.	Annual Annual

The DON Enterprise IT Controls Guidance enhances and supplements the NIST SP 800-53 Rev.4 security controls based on Financial Statement Auditor best practices.

Overlap Between Financial Audit and Cybersecurity



Cybersecurity → RMF → NIST SP 800-53 ← FISCAM ← Financial Audit

To support transition to RMF of financial systems, apply the FM Overlay (critical security controls for a financial audit) to manage and implement controls once to satisfy both cybersecurity and financial audit requirements

Navy Methodology for Integration of RMF and Financial Management (FM) Overlay

	STEP 1 CATEGORIZE Systems	STEP 2 SELECT Security Controls	STEP 3 IMPLEMENT Security Controls	STEP 4 ASSESS Security Controls	STEP 5 AUTHORIZE Information Systems	STEP 6 MONITOR Security Controls
						
RMF Process	• Identify FM System Confidentiality Integrity Availability (C-I-A) • Categorize system to CNSSI 1253 and NIST 800- 53 rev4	• Select baseline control set and applicable overlays (e.g. FM for audit relevant systems)	• Implement tailored control sets • Prepare the POAM with Navy architecture	• Assess tailored control set • SCA writes Security Assessment Report • Remediate preliminary findings	Program assemble RMF Package ↓ ***Program / Echelon II submit RMF package for FM Endorsement memo*** ↓ Authorizing Official (AO) Authorize System	• Determine impact of changes to system and environment • & assess security controls annually • AO reviews security status • System decommissioning
FM Overlay Process	FM Validator Team to play consulting role, as necessary	FM Validator Team to play consulting role, as necessary	FM Validator Team to play consulting role, as necessary	FM Validator Team works in conjunction with cyber validator to validate security controls	FM Validator Team provides endorsement memo	FM Validator Team leverages system continuous monitoring strategy for enterprise internal audit function

FM Overlay and RMF Key Takeaways

FM Overlay controls include the AC, AU, CM, and IA controls that map to FISCAM objectives and all Policy and Procedure (-1) controls

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

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 Validator is a separate team from FMP that validate FM overlay controls
- SCA relies on results of validation from FM validators to eliminate redundancy

RMF Step 5

- FMP to provide endorsement memo to NAO prior to final authorization

Overall intent is to ensure systems are in scope for an audit, implement controls critical to an audit. integrate with RMF process and adapt existing requirement.

Success Factors

1

Effective Communication

- Inter and Intra Echelon communications
- Ensure all stakeholders are engaged and represented

2

Building intellectual capital within DON/DoD

- Audit and RMF are new competencies to the DoD environment
- Knowledge sharing is critical in to building foundation of IC

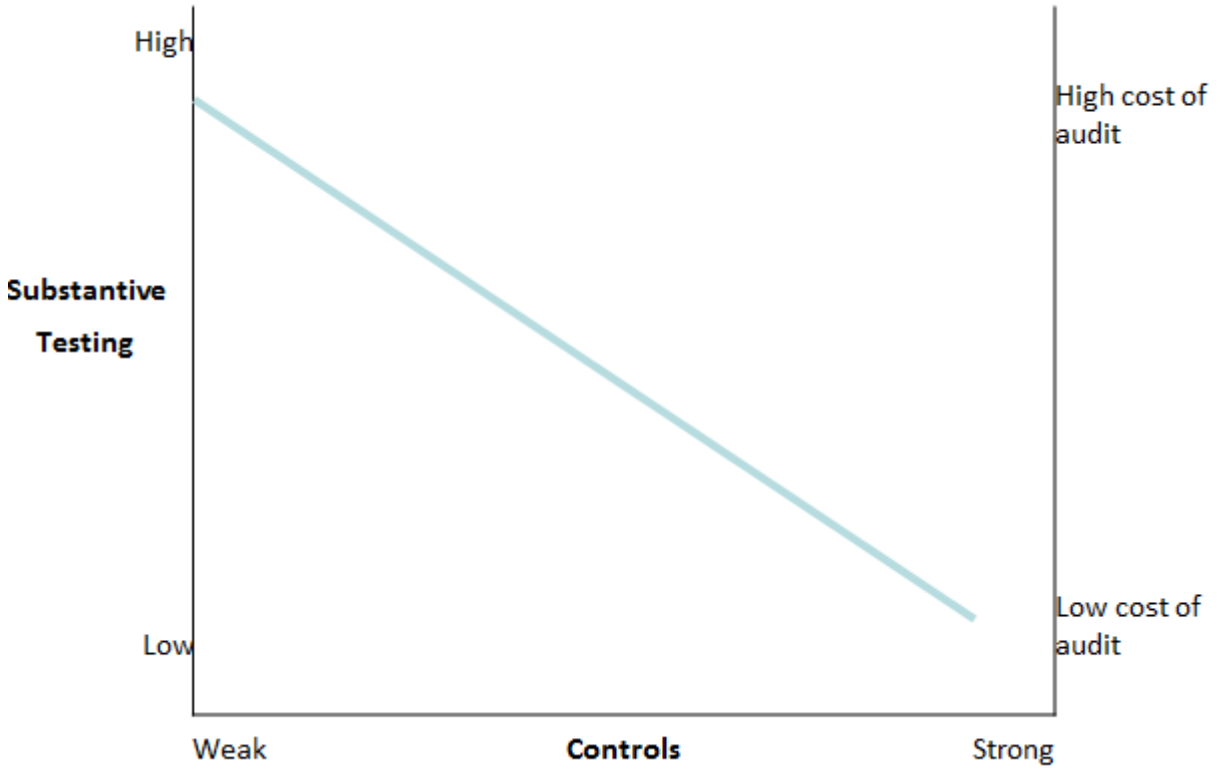
3

Ability to adapt quickly to changing environment

- Changing requirements/ Unfunded requirements
- Everything is a high priority
- Budget constraints
- System consolidations

.

Why do we care?



Auditor can gain reasonable assurance anywhere on that line,
Where do you think DoD should be?

Questions?