Lunch n Learn: 11 APR 2018

Risk Management Framework – KISS
‘Keep it Simple Security’ for RMF

- Session will start at 1230 EDT (1130 CDT).
- Audio will be through DCS – there will be a sound check 30 minutes prior to the session. Everyone but the presenter is muted
- Audio will also available via Dial-In starting at approximately Noon EDT
  - Call (712) 770-4700, Access Code: 329063#
- Download the Presentation:
  - Click on the Bold Arrow pointing downward just below the lower left hand corner of the presentation
- Questions are welcome during the session, please type them into the DCS Chat Window

Alex Basco, Moderator
Professor, Contract Management
703-805-3343
Alex.Basco@dau.mil

Jane Bernat, Contractor
SP Cybersecurity Lead
Integrated Personnel and Pay System - Army (IPPS-A)
571-367-9021

Dr. Michael Santens
Professor, Contract Management
703-805-3776
Michael.Santens@dau.mil

Lunch n Learn: 11 APR 2018
Risk Management Framework – KISS
‘Keep it Simple Security’ for RMF

Defense Acquisition University

Foundational Learning Workflow Learning Performance Learning

Jane Bernat, Contractor
SP Cybersecurity Lead
Integrated Personnel and Pay
System - Army (IPPS-A)
571-367-9021

Dr. Michael Santens
Professor, Contract Management
703-805-3776
Michael.Santens@dau.mil

Value Proposition – Taking the “Risk” out of RMF

- What Is RMF?
  - Risk Managed Framework is a methodology developed by the National Institute of Standards and Technology to implement Federal Information Security requirements and provide a framework to assess and authorize federal information systems to operate
- How Do I Reduce the Cost and Time to Implement and Maintain?
  - Implement DoD Tier 1 and Organizational Tier 2 Inheritance

3-Year Per System Savings – w/ Tier 1/2 Inheritance Implemented

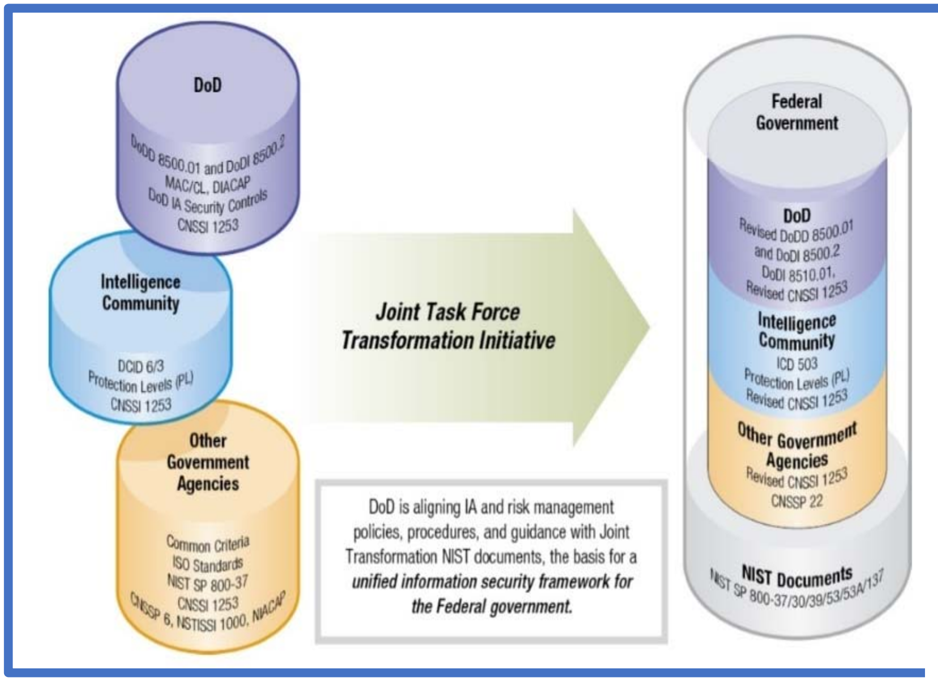
Calculated based on # of systems in the Organizations Portfolio

Programs Savings				
1	10	30	60	90
$ 861,296	$8.6M	$25.8M	$51.7M	$77.5M

Value Proposition - Re-purpose cost savings realized from implementation of effective inheritance to fund continuous monitoring tools creating additional savings

A Little History Lesson – How did we get here?

Federal and DoD Transition to RMF

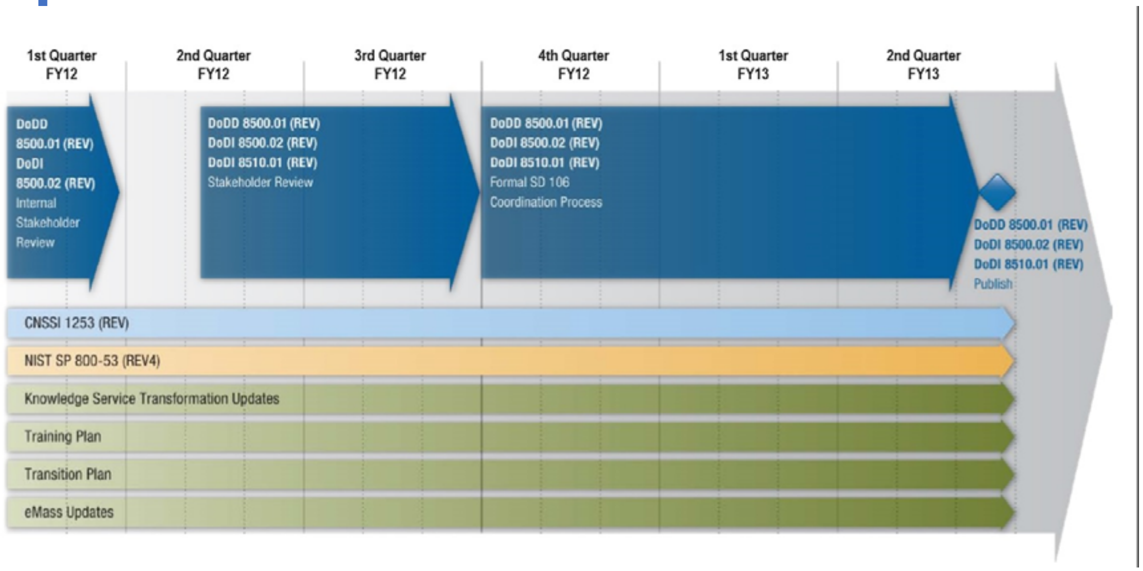


DoD is aligning IA and risk management policies, procedures, and guidance with Joint Transformation NIST documents, the basis for a *unified information security framework for the Federal government.*

Extracted from DIACAP to Risk Management Framework (RMF) Transformation DoD Brief Oct 2012

Goal - Align Information Security Compliance across the Federal Government

Goal – Build the DoD Policy Framework and Implementation Strategy to Implement Compliance



DoD Transition to RMF

- **Key Concepts – Implementing Security Controls**
  - **RMF is a *6 Step Process* – Categorize, Select Controls, Implement, Assess, Authorize and Monitor**
  - Significant change in Security Control Set
    - MAC II DIACAP System (**106 Controls**) – Moderate RMF System (**403 Controls**)
    - Increased granularity standardizes implementation across the DoD Enterprise
  - Implements ***Reciprocity*** – Authorizing Officials agree to accept each other's results
  - Implements ***Inheritance*** – Controls may be "inherited" from common providers – no re-testing required by the Information System Owner (ISO)
    - For a Moderate System DoD (Tier I) provides 420 Assessment Procedures for Inheritance
  - Continuous Monitoring or ongoing assessment – Replace the 3-year ATO cycle
- **Centrally Managed and Tracked through eMASS**
  - Implementation Plan – Overall implementation Status of Each Control
  - Risk Assessment – Documents the risk and recommendations associated with each Non-Compliant Control
  - Plan of Action & Milestones – One for each non-compliant finding mapped to the associated control – may be more than one mapped to a single control
  - Security Control – Enter test results for each assessment procedure associated with a control – number of assessment procedures varies from 1-28

Why is the DoD Transition to RMF so hard?

DIACAP vs RMF

FOCUS IS ON THE SYSTEM

DIACAP Compliance Check

Are you compliant with these controls?

□ Yes

☑ No

STOP

Costs to the Information System Owner

-- Additional Manpower to support assessment procedures

-- Additional ISSO time to research, input, and resolve test results

-- Additional IV&V time to evaluate results

-- Non compliant findings cost more – add POA&M support costs

DIACAP – 106 Controls
161 Assessment Procedures
267 Entries

FOCUS IS ON THE ORGANIZATION

Risk Management Framework

Are you compliant with these controls?

□ Yes

☑ No

What is the **Risk**? Consider:

Vulnerability Level (includes STIG findings)
Associated Threats
Likelihood of Exploitation
Compensating Controls and Mitigations

What is the **Residual Risk**? What is my organization's risk tolerance? What is my risk tolerance?

Risk Accepted

GO

RMF – 403 Controls
1643 Assessment Procedures
2046 Entries

~4x
> 10x
~7.5x

Increase in Level of Effort and Increase in the "unknown" Drive Up Contracting Costs

Building An RMF Package – Categorize

RMF Step 1 Categorize
ISSO-ISSM-SCA-AO

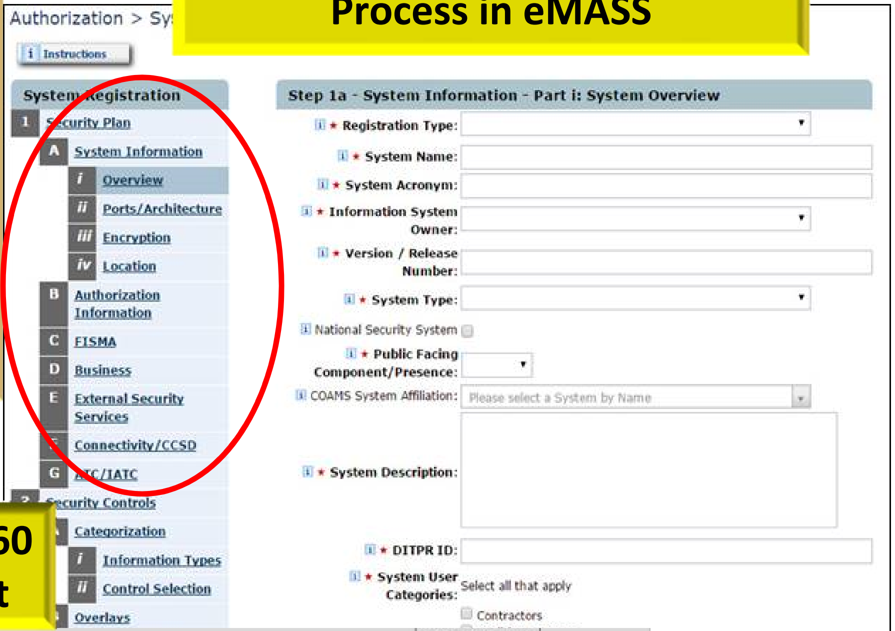
~60 hours

Minimal Level of Effort – Use of a well defined template process supports follow on actions, ensuring consistent categorization and control selection across the organization.

Action – Build Initial RMF Package in eMASS
ISSO

Organizational Strategy – Define standard sources of information – ex. Standardize responses for completion of System Details Section

Complete System Registration Process in eMASS



Step 1a - System Information - Part i: System Overview

* Registration Type:

* System Name:

* System Acronym:

* Information System Owner:

* Version / Release Number:

* System Type:

National Security System □

* Public Facing Component/Presence:

COAMS System Affiliation: Please select a System by Name

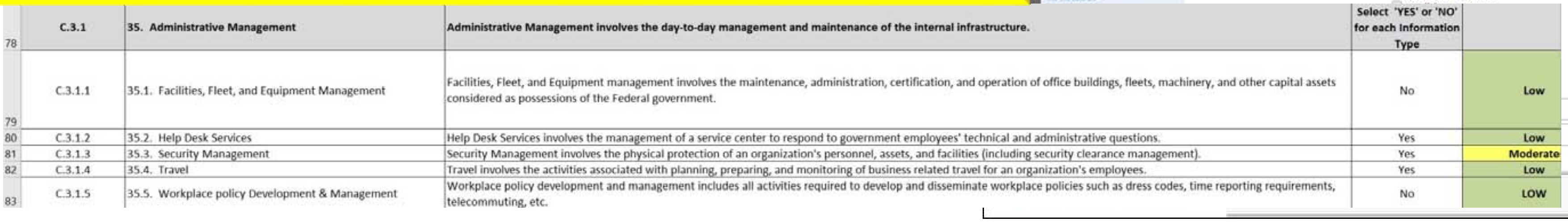
* System Description:

* DITPR ID:

* System User Categories: Select all that apply

□ Contractors

Using a Standard Information Survey Mapped to NIST SP 800-60 ensures all organizational information systems are consistent



78	C.3.1	35. Administrative Management	Administrative Management involves the day-to-day management and maintenance of the internal infrastructure.	Select 'YES' or 'NO' for each Information Type	
79	C.3.1.1	35.1. Facilities, Fleet, and Equipment Management	Facilities, Fleet, and Equipment management involves the maintenance, administration, certification, and operation of office buildings, fleets, machinery, and other capital assets considered as possessions of the Federal government.	No	Low
80	C.3.1.2	35.2. Help Desk Services	Help Desk Services involves the management of a service center to respond to government employees' technical and administrative questions.	Yes	Low
81	C.3.1.3	35.3. Security Management	Security Management involves the physical protection of an organization's personnel, assets, and facilities (including security clearance management).	Yes	Moderate
82	C.3.1.4	35.4. Travel	Travel involves the activities associated with planning, preparing, and monitoring of business related travel for an organization's employees.	Yes	Low
83	C.3.1.5	35.5. Workplace policy Development & Management	Workplace policy development and management includes all activities required to develop and disseminate workplace policies such as dress codes, time reporting requirements, telecommuting, etc.	No	LOW

Source: RMF Knowledge Service, eMASS User Guide, NIST 800-60, FIPS 199

Building An RMF Package – Select Control Baseline

~40 hours

RMF Step 2 – Select Controls
ISSO-ISSM-SCA-AO
Overlays/NSS/Financial/ Privacy

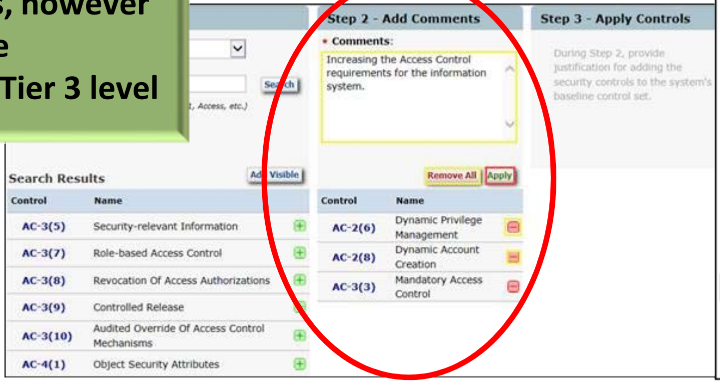
Total number of controls in a package drives level of effort for subsequent steps – Level of Effort can be managed through use of common controls – For example Privacy Families add 177 tests, however ~120 of these can be standardized/inherited at the Tier 3 level

Action – ISSO builds categorization and selects control baseline in eMASS based on categorization

Organizational Strategy – Use a standard information type survey (Army has a good one) and standard format for AO categorization memo including rationale and defining required overlays – details are important to follow on steps

Examples (controls/assessment procedures):
MMM – 403/1640
MMM w/Privacy – 453/1894
MMM w/Privacy/Financial 746/2650

Categorization determines control selection



Search Results

Control	Name
AC-3(5)	Security-relevant Information
AC-3(7)	Role-based Access Control
AC-3(8)	Revocation Of Access Authorizations
AC-3(9)	Controlled Release
AC-3(10)	Audited Override Of Access Control Mechanisms
AC-4(1)	Object Security Attributes

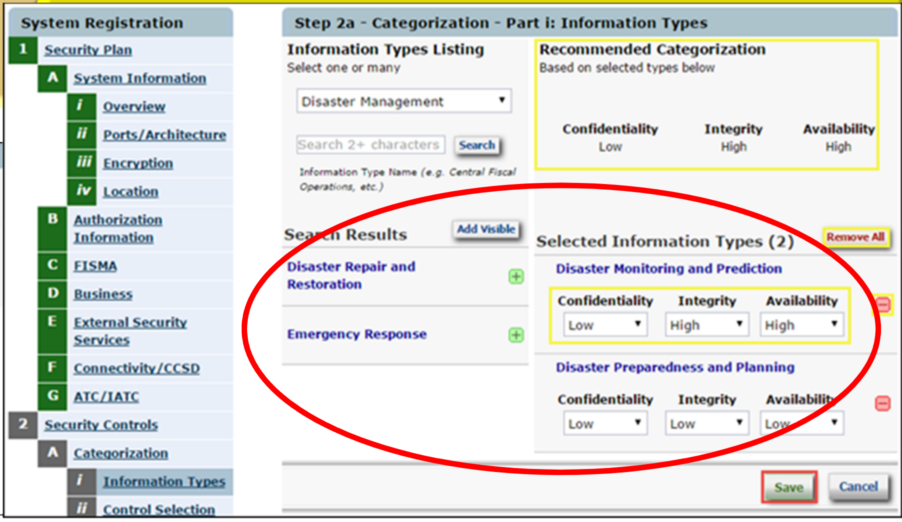
Step 2 - Add Comments

* Comments: Increasing the Access Control requirements for the information system.

Control	Name
AC-2(6)	Dynamic Privilege Management
AC-2(8)	Dynamic Account Creation
AC-3(3)	Mandatory Access Control

Step 3 - Apply Controls

During Step 2, provide justification for adding the security controls to the system's baseline control set.



Step 2a - Categorization - Part i: Information Types

Information Types Listing
Select one or many

Disaster Management

Search 2+ characters

Information Type Name (e.g. Central Fiscal Operations, etc.)

Search Results

Disaster Repair and Restoration

Emergency Response

Recommended Categorization
Based on selected types below

Confidentiality	Integrity	Availability
Low	High	High

Selected Information Types (2)

Disaster Monitoring and Prediction

Confidentiality	Integrity	Availability
Low	High	High

Disaster Preparedness and Planning

Confidentiality	Integrity	Availability
Low	Low	Low

Source: RMF Knowledge Service, eMASS User Guide, NIST 800-60, FIPS 199

Building An RMF Package – Implement Controls

RMF Step 3 – Implement System Owner/Organization – ISSO advices and investigates

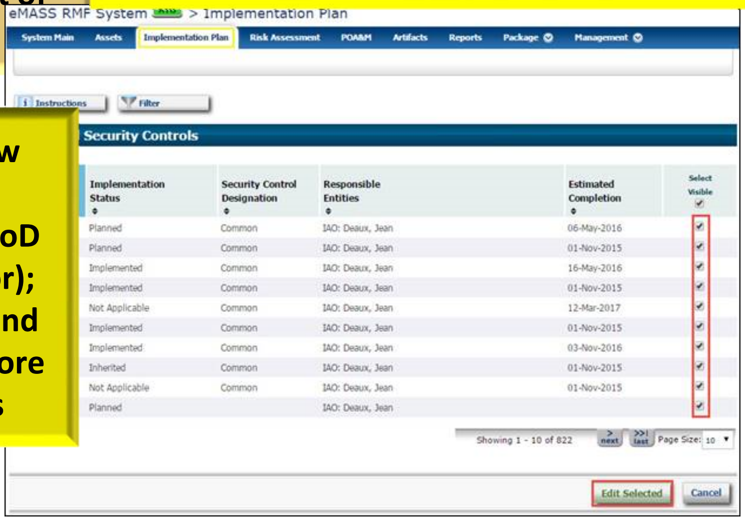
~1 hour per AP (ISSO)

Information System Owner is critical to this step – current RMF methods are asking the ISO to take responsibility for the entire control set – a systemic breakdown of RMF controls mapped to the organizational level responsible for their implementation allow system owners to focus on technical implementation and control overall costs for the RMF process. Establishing and mandating inheritance from a DoD Tier 1 SOR removes 25% of the assessment procedures from the ISO's effort.

Action – ISSO works with ISO, Organization, Hosting Environments to identify supporting documents, evidence, etc.

Organizational Strategy – Define a standard set of DoD/Component/Organizational policies, processes and procedures mapped to RMF controls to be used by ISSO to determine method of implementation. Identify common controls and develop SORs directing their use in system contracting documents to standardize assessment of organizational practices.

Implementation Plan documents whether A control is implemented, not applicable, or planned; assigns responsibility for implementation and identified inherited controls – It serves as a guide for Building a self assessment plan and forms the System Security Plan for AO Approval



Implementation Status	Security Control Designation	Responsible Entities	Estimated Completion	Select Visible ☑
Planned	Common	IAO: Deaux, Jean	06-May-2016	☑
Planned	Common	IAO: Deaux, Jean	01-Nov-2015	☑
Implemented	Common	IAO: Deaux, Jean	16-May-2016	☑
Implemented	Common	IAO: Deaux, Jean	01-Nov-2015	☑
Not Applicable	Common	IAO: Deaux, Jean	12-Mar-2017	☑
Implemented	Common	IAO: Deaux, Jean	01-Nov-2015	☑
Implemented	Common	IAO: Deaux, Jean	03-Nov-2016	☑
Inherited	Common	IAO: Deaux, Jean	01-Nov-2015	☑
Not Applicable	Common	IAO: Deaux, Jean	01-Nov-2015	☑
Planned		IAO: Deaux, Jean		☑

Showing 1 - 10 of 822

Key Opportunity to identify and review inheritance options – these include identification of a source package for DoD Tier 1 (should be specified to contractor); identification of hosting environment and organizational inheritance – manual (more work and more risk) or through SORs

Source: RMF Knowledge Service, eMASS User Guide, NIST 800-53

Building An RMF Package - Assessment

RMF Step 4 – Assess
ISSO/ISSM/SCA-AO

~2 hour per AP (ISSO)
~1 hour per AP (SCA)

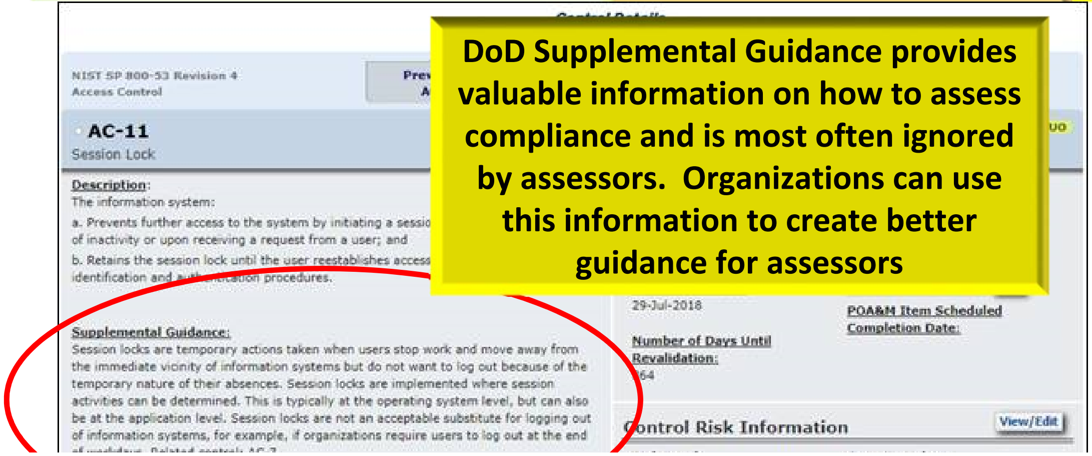
Heavy lift for the ISSO-ISSM-SCA Team. For each assessment procedure not inherited, the ISSO gathers evidence, writes a detailed test result directly citing the source used to verify, uploads the test result into eMASS, uploads evidence, maps the evidence, writes a POA&M for N/C controls. An independent SCA-V team bases fee on the number of assessment procedures and the number of components to be tested. For each non-inherited AP, they review the test results, verify them against the evidence and determine if they are correctly assessed. They complete a risk assessment based on non-compliant controls

Action – ISSO assembles supporting documentation, conducting testing, interviews, documentation reviews to determine compliance/non-compliance/applicability for each assessment procedure. SCA-V provides independent review/verification of each result

Organizational Strategy – Mapping of control providers through inheritance narrow the controls assessed to those directly attributable to the ISO. Overarching organizational controls are assessed once – consistently and "inherited" by all information systems – natural check and balances are used to ensure compliance

Assessor's toolkit:
DoD Policies (Tier 1)
Component Policies (Service, DHA, DLA, etc) – Tier 2
Organizational Policies – Tier 3
Hosting Environment – Technical/Policy – Tier 3
Information System Specific – processes, procedures, documentation, technical controls, STIGs, system design

"Organizations defining the Assessor's toolkit upfront will reduce the vendor's risk, standardize security baselines, and substantially reduce both cost and risk while level setting security implementation across the AO's portfolio."



NIST SP 800-53 Revision 4
Access Control

AC-11
Session Lock

Description:
The information system:
a. Prevents further access to the system by initiating a sessio
of inactivity or upon receiving a request from a user; and
b. Retains the session lock until the user reestablishes access
identification and authentication procedures.

Supplemental Guidance:
Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related controls: AC-7.

29-Jul-2018

POA&M Item Scheduled Completion Date:

Number of Days Until Revalidation:
364

Control Risk Information

DoD Supplemental Guidance provides valuable information on how to assess compliance and is most often ignored by assessors. Organizations can use this information to create better guidance for assessors

Most Time consuming, highest risk, most subjective, and least "managed" component of the RMF process – fully reliant on the skill and experience of the assessor and validator.

Biggest opportunity for cost savings and reduction – standardizing through inheritance saves 3 hours per procedure per system

Perhaps we missed something…….

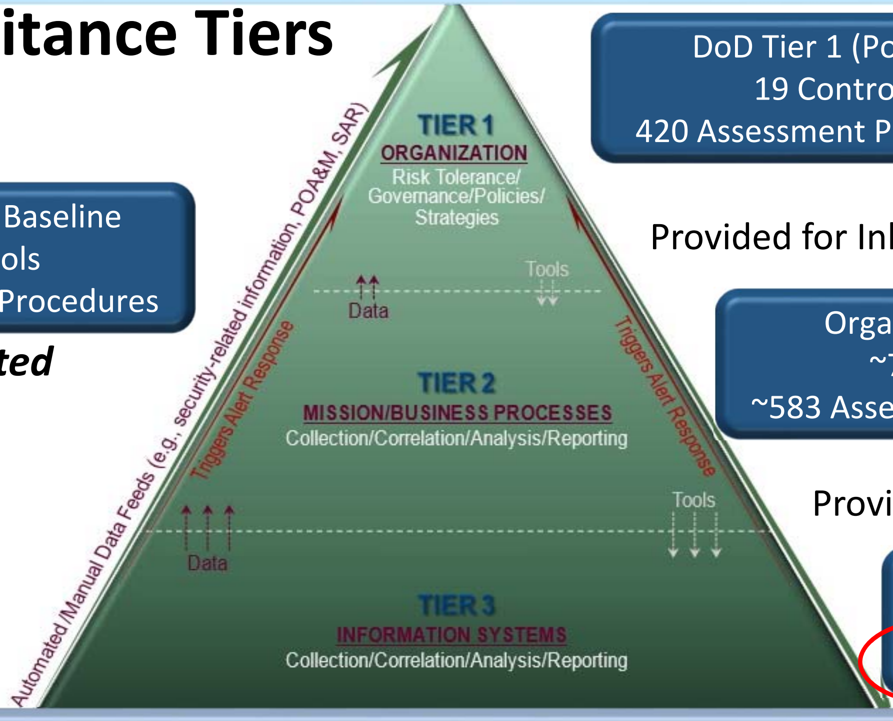
Mapping each control to the level of the organization responsible for its implementation

INHERITANCE!!!

Inheritance – A Key Concept in the Value Proposition

Level of effort without Tier 2 Inheritance - 4557 hours
With Tier 2 Inheritance - 2607 hours

DoD Inheritance Tiers



TIER 1
ORGANIZATION
Risk Tolerance/
Governance/Policies/
Strategies
Tools
Data
TIER 2
MISSION/BUSINESS PROCESSES
Collection/Correlation/Analysis/Reporting
Tools
Data
TIER 3
INFORMATION SYSTEMS
Collection/Correlation/Analysis/Reporting
Automated /Manual Data Feeds (e.g., security-related information, POA&M, SAR)
Triggers Alert Response
Triggers Alert Response

RMF Moderate Baseline
403 Controls
1643 Assessment Procedures

DoD Tier 1 (Policies)
19 Controls
420 Assessment Procedures

Provided for Inheritance By

Organization Tier 2
~72 Controls
~583 Assessment Procedures

Provided for Inheritance By

Information System Tier 3
~312 Controls
~640 Assessment Procedures

Bottom Line – A properly implemented Inheritance Strategy can reduce the Manhours required to Assess an Information System by ~60%

Inheritance of DoD Tier 1 Controls Already Provide a 25% reduction

Controls are assessed, authorized and monitored by the level of the organization providing the control. Controls provided by Tier 1 and 2 are "inherited" by Tier 3.

Triangle Tier 1-3 Graphic Extracted from NIST

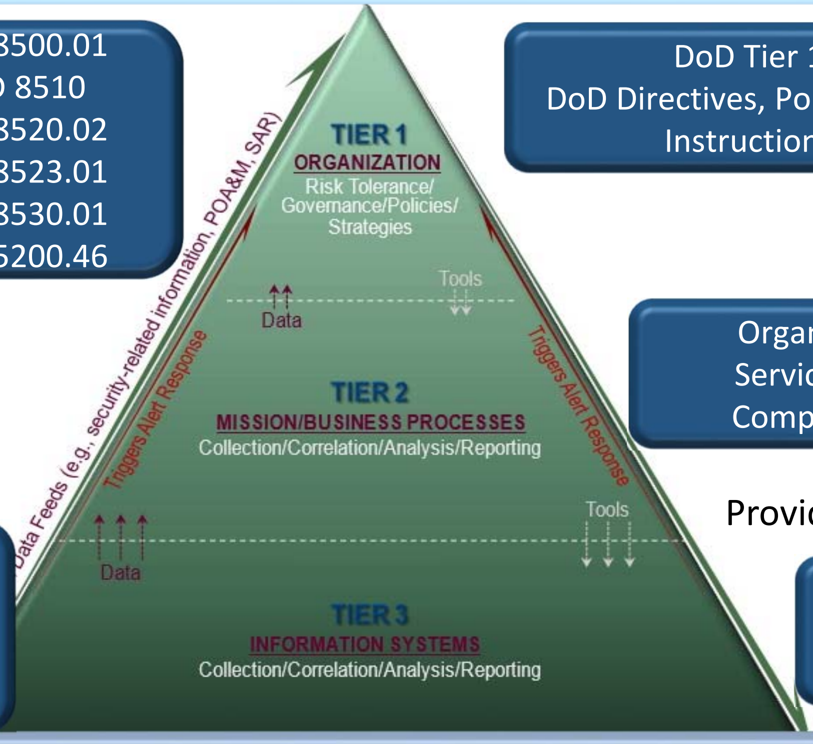
Mapping Controls to Organizational Implementation

Standardize and Provide Specific Guidance to contractors on The documents to be used to support RMF Assessments

DoD 8500.01
DoD 8510
DoD 8520.02
DoD 8523.01
DoD 8530.01
DoD 5200.46

AR-25-1
AR-25-2
AR-600-20
AR-380-53
32 CFR Part 505
Army Data Spillage

Organizational Polices
PIAs and SORNs
Standard Contract Language
Organizational Processes


Data Feeds (e.g., security-related information, POA&M, SAR)
Triggers Alert Response
Triggers Alert Response
TIER 1
ORGANIZATION
Risk Tolerance/ Governance/Policies/ Strategies
Tools
Data
TIER 2
MISSION/BUSINESS PROCESSES
Collection/Correlation/Analysis/Reporting
Tools
Data
TIER 3
INFORMATION SYSTEMS
Collection/Correlation/Analysis/Reporting

DoD Tier 1
DoD Directives, Policies, and Instructions

Organization Tier 2
Service Regulations
Component Policies

Provided for Inheritance By

Information System Tier 3
Agency/Organizational Polices

Each Organizational Level Issues Policies Implementing the Security framework assessed by RMF

Triangle Tier 1-3 Graphic Extracted from NIST

An Example – Privacy Families

- 8 Privacy Families – Total of 28 Controls – Total of 177 Assessment Procedures
- Key supporting Documents – Privacy Impact Assessment (PIA) and System of Records Notice (SORN)
  - PIA and SORN formats and the required information provided in each section is consistent
  - Assessment procedure can be answered by referencing the appropriate PIA section – ex. "PIA Section 2h explicitly identifies all DoD and non-DoD organizations with whom PII is shared."
  - PIAs and SORNs are formally reviewed and approved. A signed PIA/SORN ensures the information contained in the document is compliant.
- Key Official - Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) – Consistent for every Army system – Source OSD Memo for Appointment of a SAOP for Privacy
- Current Method of RMF Package Prep – Assessed at the system level
- Proposed methods
  - Method 1 -- Create a Privacy Specific System of Record at the Tier 3 level to standardize assessments
    - Added advantage – "Inherited" controls are not "validated" during a SCA-V assessment – if the inheritance is valid, the control status is accepted – validate once use many times – for N/C controls POA&M is tracked by SOR and inherited
  - Method 2 – Create a Standard Set of Test results and provided to each system owner for import into their package
    - Risk – A standard set of test results will be validated by each SCA-V team – this subjects the same result to the "opinion" of multiple validators with the potential for multiple results to the same answer
    - For N/C controls – each system must maintain a POA&M and manually track the resolution

A Tale of Two ATOs – What Can Go Wrong

AR-2.1 Assessment Procedure
The organization documents a privacy risk management process which assesses the privacy risk to individuals..

DoD Supplemental Guidance
Organizational privacy risk management processes operate across the life cycles of all mission/business processes that collect, use, maintain, share, or dispose of PII. The tools and processes for managing risk are specific to organizational missions and resources. They include, but are not limited to, the conduct of PIAs. The PIA is both a process and the document that is the outcome of that process. OMB Memorandum 03-22 provides guidance to organizations for implementing the privacy provisions of the E-Government Act of 2002, including guidance on when PIAs are required for information systems.

TEST RESULTS System 1
Follows Army guidance provided through the Army Privacy Office. Army Privacy Regulation 32 CFR 505. System has a PIA and SORN in place providing specific guidance for meeting privacy regulations and policies. PIA Section 2g, 3f and SORN Narrative Section 4 identifies and assesses privacy risk to individuals

VALIDATOR RESPONSE
The organization was compliant with this CCI. Follows Army guidance provided through the Army Privacy Office. Army Privacy Regulation 32 CFR 505. PIA and SORN in place providing specific guidance for meeting privacy regulations and policies. Specific privacy implementation guidance also provided on the Army Privacy Program Web page. Risk management addressed in PIA Section 2g.

Successful SCA-V Assessment
ATO Granted

Assessors and Validators agreed 98% of the time

TEST RESULTS System 2
PISSM has determined this CCI compliant because the Privacy Control document identifies in paragraph 4 the privacy risk management process which assesses the privacy risk to individuals.

VALIDATOR RESPONSE
CCI-003417 DC- Organization did not document a risk management process for privacy that assessed the privacy risk to individuals from collecting, sharing, storing, transmitting, using, and disposing Personally Identifiable Information (PII)

SCA-V Assessment Suspended
Package returned for re-work after 100 controls self- assessed as compliant were invalidated by the SCA-V Team

Assessors identified only 2 controls as N/C – after assessing 40% of the controls Validators assessed 102 controls as N/C

The guidance provided by RMF documents compliance is in the PIA – System 1 used The PIA to support the assessment, linking the PIA to the control. System 2 created an Additional document but did not accurately list the document name and linked 3 additional Documents to the control – the SCA-V could not use the PIA although it was linked since The original assessor did not identify it as the basis for compliance.

The Inheritance Dividend – POA&Ms…….

One Non-Compliant Control → POA&M

A Tier 2 finding for an organization with 30 systems in their portfolio would track the issue with 1 POA&M if they were providing the N/C control for inheritance instead of 30 POA&Ms at the system level

One Representative System

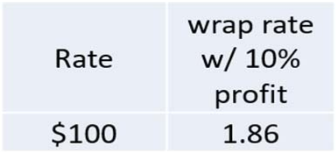
- POA&Ms are mapped to the organizational level capable of resolving the issue
- Organizational, issue driven POA&Ms are instantiated once – Resolution impacts many
- Organizational POA&Ms cost less to manage – Estimate of $1000 Annual cost to maintain each POA&M
    - Labor hours expended annually tracking, researching, meeting time, reporting, etc
    - Today – 30 POA&Ms generated for an organizational issue -- $30K to maintain
    - Under RMF – 1 POA&M generated – issue specific, assigned to the POC capable of executing a resolution -- $1K to maintain
- Once resolved, the resolution is inherited in eMASS – Implementation of Continuous Monitoring/Continuous Resolution

Benefits: Reduced Cost, Risk Mapped to Organizational Level, Information System Owner’s focus on System Level Vulnerabilities, Provides the foundation for Policy/Procedural Alignment with Risk
*** Steady Reduction in the number of “Testable Actions” in A&A efforts ***

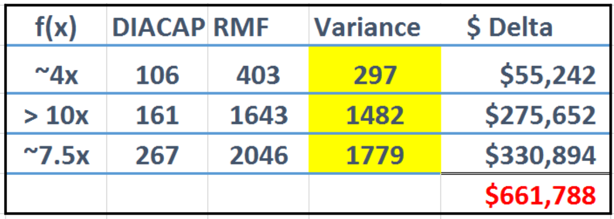
Creating Checks and Balances for Inheritance

- Inheritance Approval is controlled by the SOR Owner and can be revoked
- Careful selection of the specific Assessment Procedures provided will create a “shared” implementation between SOR owners and Information System Owners
- Organizing SORs around s specific organizational policy or practice allows common control providers to tailor inheritance for each information system – develop multiple SORs
  - For example – Human Resources Command uses a single SORN for multiple PII systems in its portfolio – An SOR validated through the SORN, approved system PIAs, and standard Army regulations could be built with the caveat that a system requesting inheritance must submit their approved PIA to add to the package. The SOR owner would not grant inheritance until the PIA is received – SOR owner would be able to track 2 year updated requirement, revoking inheritance for any system not keeping their PIA current
- Use the Assessment Procedures to create check and balance – DoD breaks down controls into CCIs – map CCIs to ISO and the organization as appropriate
  - Ex. PL-2 (Develop a System Security Plan) consists of 19 CCIs
    - 3 are inherited from DoD Tier 1
    - CCI 3049 - The organization develops a security plan for the information system is met through eMASS and could be inherited
    - CCI 3051 - The organization's security plan for the information system explicitly defines the authorization boundary for the system is provided by the ISO and should be assessed by the system ISSO
  - Mapping CCIs (Assessment Procedures) correctly allows ISOs to demonstrate compliance to an organizational policy without assessing the compliance of the policy itself – this would be completed at the Tier 2 or Tier 3 level

Cost Drivers for RMF Implementation



Rate	wrap rate w/ 10% profit
$100	1.86

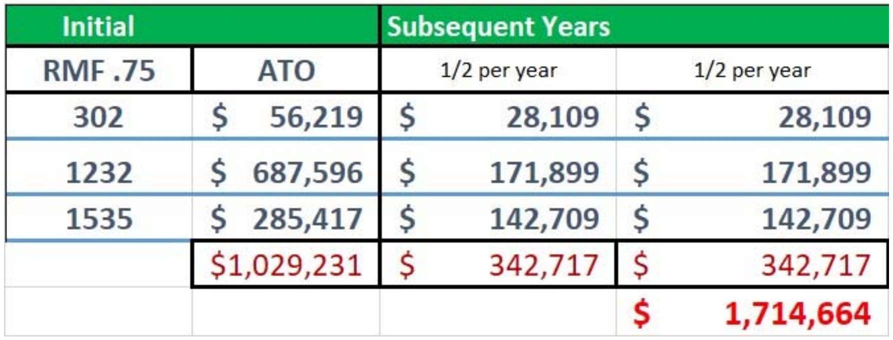


f(x)	DIACAP	RMF	Variance	$ Delta
~4x	106	403	297	$55,242
> 10x	161	1643	1482	$275,652
~7.5x	267	2046	1779	$330,894
				$661,788

Difference in transitioning from DIACAP to RMF

3-Year Cost – No Inheritance
$2,133,420 for one program

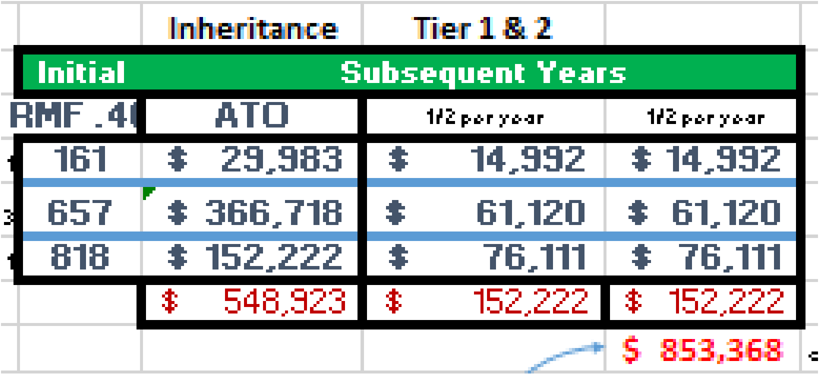
3-year DIACAP cycle
$1,471,632 for one program



Initial		Subsequent Years	
RMF .75	ATO	1/2 per year	1/2 per year
302	$ 56,219	$ 28,109	$ 28,109
1232	$ 687,596	$ 171,899	$ 171,899
1535	$ 285,417	$ 142,709	$ 142,709
	$1,029,231	$ 342,717	$ 342,717
			$ 1,714,664

A representative RMF program w/ DoD Tier 1 inheritance

= **$1,714,664 for one program**



	Inheritance	Tier 1 & 2	
Initial		Subsequent Years	
RMF .4	ATO	1/2 per year	1/2 per year
161	$ 29,983	$ 14,992	$ 14,992
657	$ 366,718	$ 61,120	$ 61,120
818	$ 152,222	$ 76,111	$ 76,111
	$ 548,923	$ 152,222	$ 152,222
			$ 853,368

A representative RMF program w/Tier 1/2 inheritance

= **$853,368 for one program**

Summary

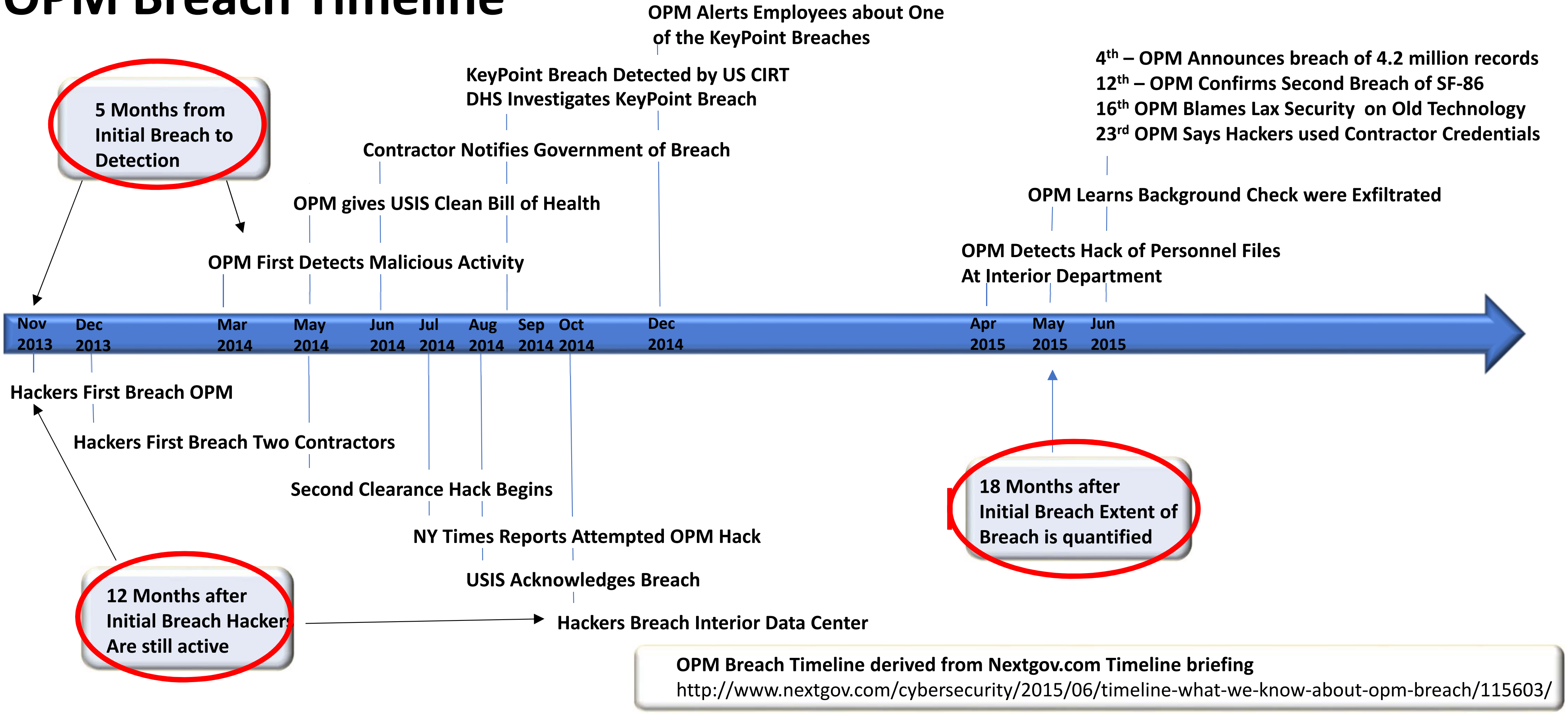
- Inheritance is an effective tool to accomplish the following
  - Map controls to the organizational entity responsible for their implementation
  - Standardize assessment and implementation of organizational controls – Assess once and results are consistently applied across all of the organization's systems – AOs have the ability to discern organizational risk from individual system risk
  - Provide standard guidance to contractors executing RMF assessments to drive down cost through elimination of contract risk – for example, identifying a standard inheritance package for DoD Tier 1 controls (~20-25% of the total number of assessment procedures in a package)
  - Implement Continuous Monitoring – tie maintenance of Systems of Record to policy and procedure updates – use control assessments and POA&Ms to track deficiencies and schedule required reviews/updates
    - Provide continual updates to each system's package when organizational control compliance is updated, officials change, or new policies are identified and implemented – for example appointment of a new AO. Using inheritance, each system would automatically have the new AO's appointment letter and information updated to their package through a single update of the associated organizational control.
- The cost of building and maintaining one or more SORs is recovered after inheritance is provided to 2 systems. Successive inheritance is direct cost savings.

The “Holy Grail” – Continuous Monitoring

Replace the current “snapshot in time” 3-year Certification and Accreditation (C&A) Cycle with Ongoing Assessment – Quantify risk in real time

Why Does Continuous Monitoring Matter? The OPM Breach was Preventable

OPM Breach Timeline



OPM Alerts Employees about One of the KeyPoint Breaches

KeyPoint Breach Detected by US CIRT
DHS Investigates KeyPoint Breach

Contractor Notifies Government of Breach

OPM gives USIS Clean Bill of Health

OPM First Detects Malicious Activity

4th – OPM Announces breach of 4.2 million records
12th – OPM Confirms Second Breach of SF-86
16th OPM Blames Lax Security on Old Technology
23rd OPM Says Hackers used Contractor Credentials

OPM Learns Background Check were Exfiltrated

OPM Detects Hack of Personnel Files At Interior Department

5 Months from Initial Breach to Detection

Nov 2013 · Dec 2013 · Mar 2014 · May 2014 · Jun 2014 · Jul 2014 · Aug 2014 · Sep 2014 · Oct 2014 · Dec 2014 · Apr 2015 · May 2015 · Jun 2015

Hackers First Breach OPM

Hackers First Breach Two Contractors

Second Clearance Hack Begins

NY Times Reports Attempted OPM Hack

USIS Acknowledges Breach

Hackers Breach Interior Data Center

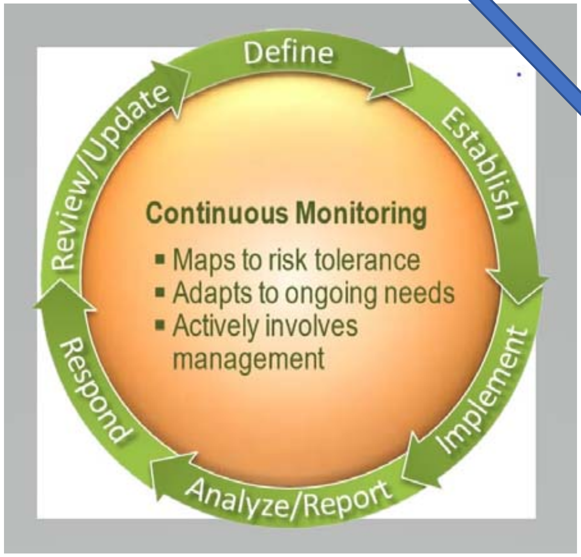
12 Months after Initial Breach Hackers Are still active

18 Months after Initial Breach Extent of Breach is quantified

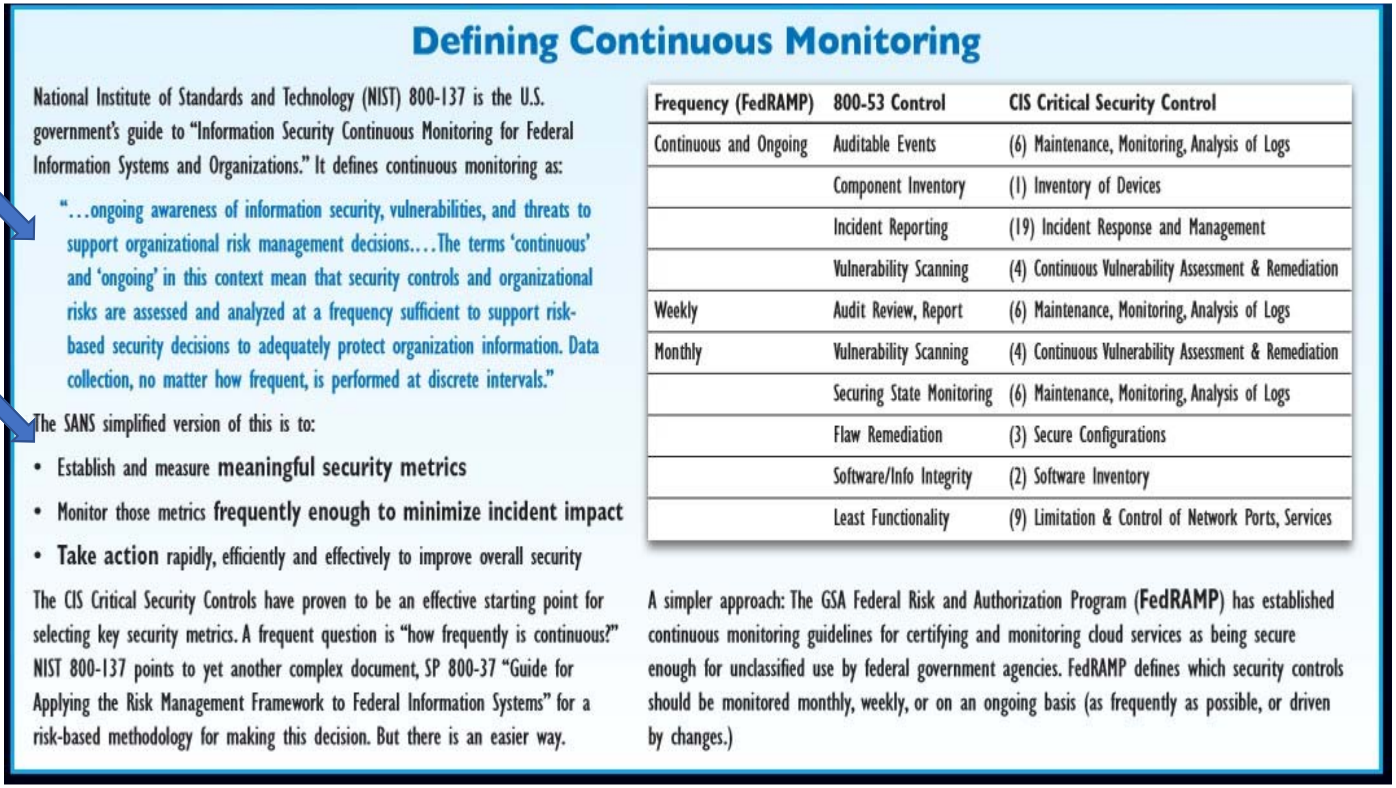
OPM Breach Timeline derived from Nextgov.com Timeline briefing
http://www.nextgov.com/cybersecurity/2015/06/timeline-what-we-know-about-opm-breach/115603/

What is Continuous Monitoring?

- Step 6 of the Risk Management Framework
- NIST Definition
- SANS Definition



Extracted from NIST SP 800-137



Defining Continuous Monitoring

National Institute of Standards and Technology (NIST) 800-137 is the U.S. government's guide to "Information Security Continuous Monitoring for Federal Information Systems and Organizations." It defines continuous monitoring as:

> "…ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.…The terms 'continuous' and 'ongoing' in this context mean that security controls and organizational risks are assessed and analyzed at a frequency sufficient to support risk-based security decisions to adequately protect organization information. Data collection, no matter how frequent, is performed at discrete intervals."

The SANS simplified version of this is to:

- Establish and measure **meaningful security metrics**
- Monitor those metrics **frequently enough to minimize incident impact**
- **Take action** rapidly, efficiently and effectively to improve overall security

The CIS Critical Security Controls have proven to be an effective starting point for selecting key security metrics. A frequent question is "how frequently is continuous?" NIST 800-137 points to yet another complex document, SP 800-37 "Guide for Applying the Risk Management Framework to Federal Information Systems" for a risk-based methodology for making this decision. But there is an easier way.

Frequency (FedRAMP)	800-53 Control	CIS Critical Security Control
Continuous and Ongoing	Auditable Events	(6) Maintenance, Monitoring, Analysis of Logs
	Component Inventory	(1) Inventory of Devices
	Incident Reporting	(19) Incident Response and Management
	Vulnerability Scanning	(4) Continuous Vulnerability Assessment & Remediation
Weekly	Audit Review, Report	(6) Maintenance, Monitoring, Analysis of Logs
Monthly	Vulnerability Scanning	(4) Continuous Vulnerability Assessment & Remediation
	Securing State Monitoring	(6) Maintenance, Monitoring, Analysis of Logs
	Flaw Remediation	(3) Secure Configurations
	Software/Info Integrity	(2) Software Inventory
	Least Functionality	(9) Limitation & Control of Network Ports, Services

A simpler approach: The GSA Federal Risk and Authorization Program (**FedRAMP**) has established continuous monitoring guidelines for certifying and monitoring cloud services as being secure enough for unclassified use by federal government agencies. FedRAMP defines which security controls should be monitored monthly, weekly, or on an ongoing basis (as frequently as possible, or driven by changes.)

Extracted from SANS Top 20 Critical Control Poster 2016

Inheritance Impact on Continuous Monitoring

Collecting Meaningful Security Data – Monitoring the Right Stuff

Security monitoring has no value on its own unless it leads to meaningful action to prevent or reduce damage from cyber attacks. More prevention, faster detection, and more accurate response require measuring different CIS Critical Security Controls to reduce vulnerabilities, detect and mitigate attacks, and optimize incident response and restoration. SANS has mapped the Critical Controls across the CyberDefense lifecycle.

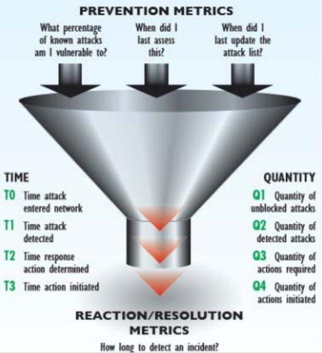
CYBER DEFENSE LIFECYCLE

CIS CRITICAL SECURITY CONTROLS

Resource Hardening	Privilege and Access Management	Attack Detection/Mitigation	Compromise Detection, Response, Recovery, and Reporting
Hardware and Software Inventory CSC1 & CSC2	Admin Privileges CSC5	Malware Defenses CSC7 & CSC8	Data Recovery CSC10
Secure Configurations CSC3, CSC9, CSC11 & CSC15	Controlled Access CSC14	Boundary Defense CSC12	Audit CSC6
Vulnerability Assessment & Application Security CSC4 & CSC18	Account Managing CSC16		Data Protection CSC13
			Incident Response CSC19

People and Processes
The Critical Security Controls include a number of security areas that focus on people and processes and are applicable across the entire lifecycle:
CSC17 – Security Skills Assessment and Training
CSC20 – Penetration Testing and Red Team Exercises

The values you measure should include both quantity and time – how quickly you detect new misconfigurations, vulnerabilites, attacks, etc. is just as important as how many there are. Similarly, business damage is minimized (and often prevented) if intrusion detection and mitigation processes can move rapidly.


PREVENTION METRICS
What percentage of known attacks am I vulnerable to?
When did I last assess this?
When did I last update the attack list?
TIME
T0 Time attack entered network
T1 Time attack detected
T2 Time response action determined
T3 Time action initiated
QUANTITY
Q1 Quantity of unblocked attacks
Q2 Quantity of detected attacks
Q3 Quantity of actions required
Q4 Quantity of actions initiated
REACTION/RESOLUTION METRICS
How long to detect an incident?

Extracted from SANS
Top 20 Critical Control Poster 2016

~65% of the RMF Assessment
Are met through documentation
Many of these are already monitored
And are excellent inheritance candidates

Type	Examples	Frequency of Update	Method of Monitoring	% of Assessment Procedures	Responsible Party
Documentation	Policies, System Documentation	Annual - Every 3 Years	External to System	~50%	Organization/ISO
Process and Procedure	Operating Procedures, Rules of Behavior, Access Procedures, Acquisition, Configuration Management	As required - Annual Review	External to System	~15%	Organization/ISO
Testing	Disaster Recovery, Incident Response, Failover	Monthly - Annual	External to System	<4%	ISO
Training	Cyber, Incident Response, System Recovery	As required - Annual Review	External to System	<3%	Organization/ISO
Technical	Configuration Settings, Security Policies	Ongoing, by exception	System Monitoring	~10%	ISO
Technical	Encryption, PKI, Network Security	Ongoing, by exception	External to System	<3%	Hosting Environment
Physical	Facilities, Utilities, Telecom, Physical Security	Ongoing, as required	External to System	~10%	Hosting Environment
Vulnerability	Threats, system flaws, patching	Ongoing, respond to emerging threat	System Monitoring	<4%	ISO
		Approximate % of Controls for Continuous Monitoring by the ISO		**10% or 160**	

Only ~10% of the RMF Assessment
Are met through technical capabilities
Integrated w/the system

Contract Strategy Considerations -PERFORMANCE

- ➢Does the program have executive-level support for Agile development?
- ➢ Is the program considered high risk?
  - o What level of risk is the government willing to accept?
- Does the current political environment drive the use of a particular contract type or vehicle?
- What is the level of contracting support?
  - o Does the KO office have standardized processes available?
  - o Are Gvmt resources available to actively manage contractor support?
  - o Imbed or centrally located at base?

Contract Strategy Considerations - SCHEDULE

- ➢Who is responsible for systems integration?
  - ➢What level of integration is required?
  - ➢What is the level of integration risk if multiple contractors conduct parallel developments?
- ➢ What is the overall development timeline?
  - What is the frequency of releases?

Contract Strategy Considerations -COST

- Can the program leverage established contract vehicles - portfolio, enterprise, or external level?
    - ➢ Are other, similar programs currently using or thinking of pursuing Agile?
- Is an Agile process well defined or already in place within the government PMO?
- Did market research (FAR Part 10) identify available qualified contractors with Agile and domain experience?
- Are GSA schedules 70 or 18-F available for use?

Summary and Clarifying Questions

Jane Bernat (Contractor) and Dr. Michael Santens (Government)

CISSP, CISM, ITILv3, & PMP CPCM, NCMA Fellow, ITILv3, CSM, MBA, & PMP