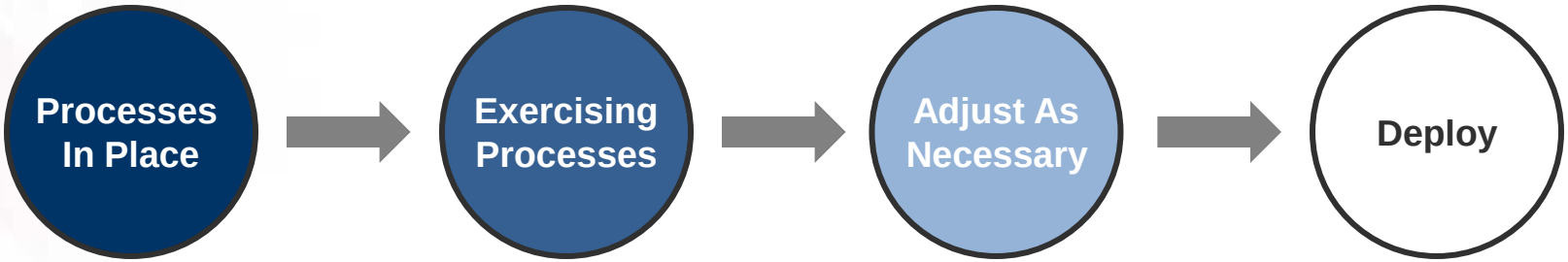
Homeland Security

Ongoing Authorization (OA)

Panel Discussion

08 August 2013
Office of the Chief Information Officer
Information Security Office

Status



Continuous Monitoring Strategy

OA Methodology

Pilot OA

Component Tailoring

Evaluate Triggers

Revise Processes

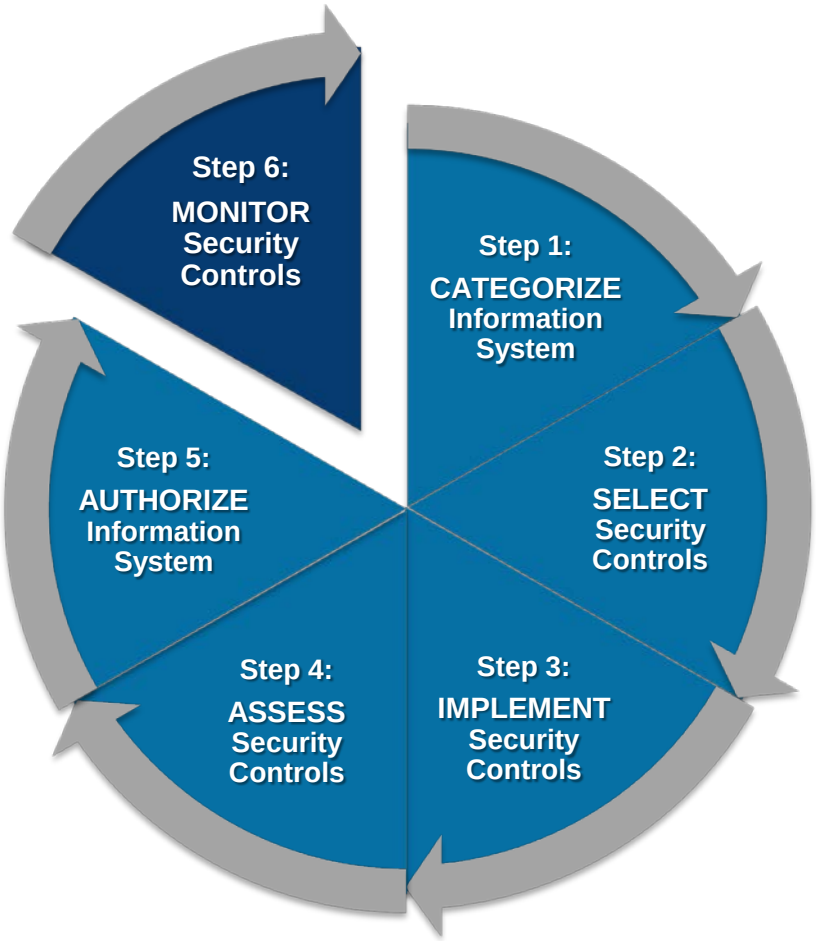
Create Supplemental Guidance

Fiscal Year 2014
(October 1, 2013)

Position within Risk Management Framework

1. Information System and Environment Changes
2. Ongoing Security Control Assessment
3. Ongoing Remediation Actions
4. Key Updates
5. Security Status Reporting
6. Ongoing Risk Determination and Acceptance

Addressed within Ongoing Authorization Methodology



Steps 1-5 addressed in DHS Security Authorization Process

System OA Eligibility

The following are required to enter the DHS OA program:

- **Components must have a(n):**
  - ✓ Robust Continuous Monitoring program
  - ✓ Signed Memorandum of Agreement (MOA)
  - ✓ OA Manager(s)
  - ✓ Operational Risk Management Board (ORMB)
  - ✓ Quality Common Control Catalogs

- **Systems must have a:**
  - ✓ ISSO with <49% collateral duties
  - ✓ Current Authority to Operate (ATO)
  - ✓ OA Recommendation Letter (baseline)
  - ✓ Control Allocation Table (CAT)

Summary Pilot Systems

Component/ System	Security Categorization (C-I-A)	Ongoing Authorization Start Date	MOA	CAT	AO Letter	Status
Immigration and Customs Enforcement (ICE)			✓			
ICE System-1	M-M-L	7/25/2013		✓	✓	Active In OA
ICE System-2	M-M-M	7/18/2013		✓	✓	Active In OA
ICE System-3	M-M-M	7/25/2013		✓	✓	Active In OA
ICE System-4	M-M-M	7/24/2013		✓	✓	Active In OA
ICE System-5	M-L-L	7/1/2013		✓	✓	Active In OA
ICE System-6	M-L-L	3/31/2013		✓	✓	Active In OA
ICE System-7	M-M-M	Pending				Preparing for OA
ICE System-8	H-M-M	Pending				Preparing for OA
ICE System-9	M-L-L	Pending				Preparing for OA
ICE System-10	M-M-L	Pending				Preparing for OA
Transportation Security Administration (TSA)			**Being Revised**			
TSA System-1	M-M-L	3/31/2013		✓	✓	Active In OA
TSA System-2	H-H-H	7/31/13		✓	✓	Active in OA
TSA System-3	H-H-H	Pending				Preparing for OA
DHS Enterprise Services (DHS HQ)			✓			
DHS HQ System -1	M-M-M	3/31/2013		✓	✓	Active In OA
US Citizenship and Immigration Services (USCIS)			✓			
USCIS System-1	H-H-H	Pending				Preparing for OA
USCIS System-2	H-H-M	Pending				Preparing for OA
USCIS System-3	M-M-L	Pending				Preparing for OA

Control Allocation Table (CAT)

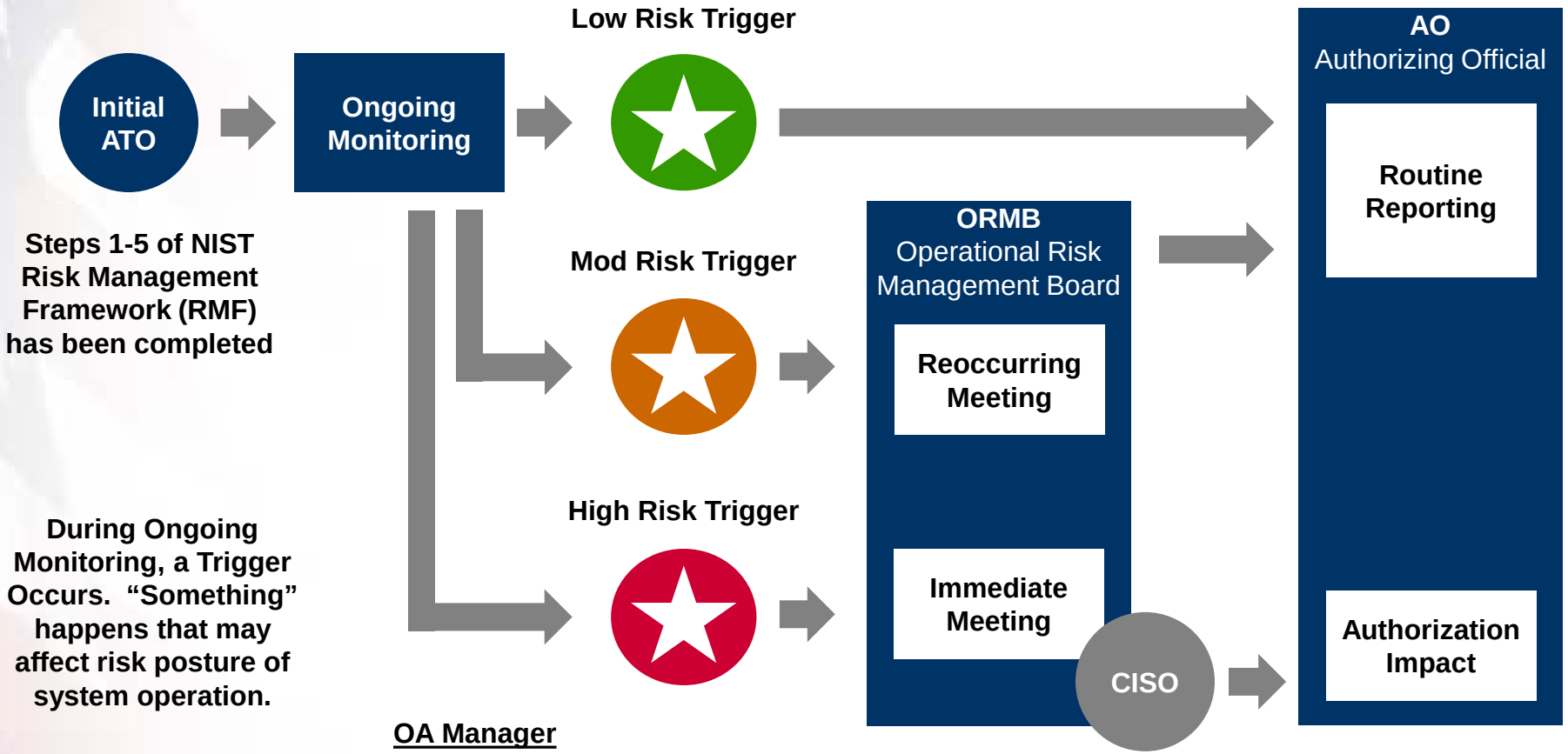
Control	Enterprise Common Control	Component Common Control	Continuous Monitoring	System Specific	Risk Accepted	POA&M	Frequency	Impact
AC-02		X			X	#3	2 Years	2 (M)
AC-19		X					4 Years	1 (H)
AC-22				X			2 Years	2 (M)
PL-06				X	X	#13	4 Years	3 (L)
RA-05	X	X	X	X			Monthly	1 (H)
SI-03	X	X	X	X			2 Years	2 (M)
Totals	**38**	**80**	**5**	**123**				

Identifies controls outside of their direct control

Outlines assessment frequency and impact

DHS Ongoing Authorization Methodology v1.4, page 3:
*"Based on findings, it may be necessary to update the **frequency** and **rigor** at which controls are assessed."*

DHS OA Process



Steps 1-5 of NIST Risk Management Framework (RMF) has been completed

During Ongoing Monitoring, a Trigger Occurs. "Something" happens that may affect risk posture of system operation.

OA Manager

- Establishes a Trigger Severity
- Considers Security Categorization
- Aligns with Risk Threshold for the System

Potential Impact Evaluated

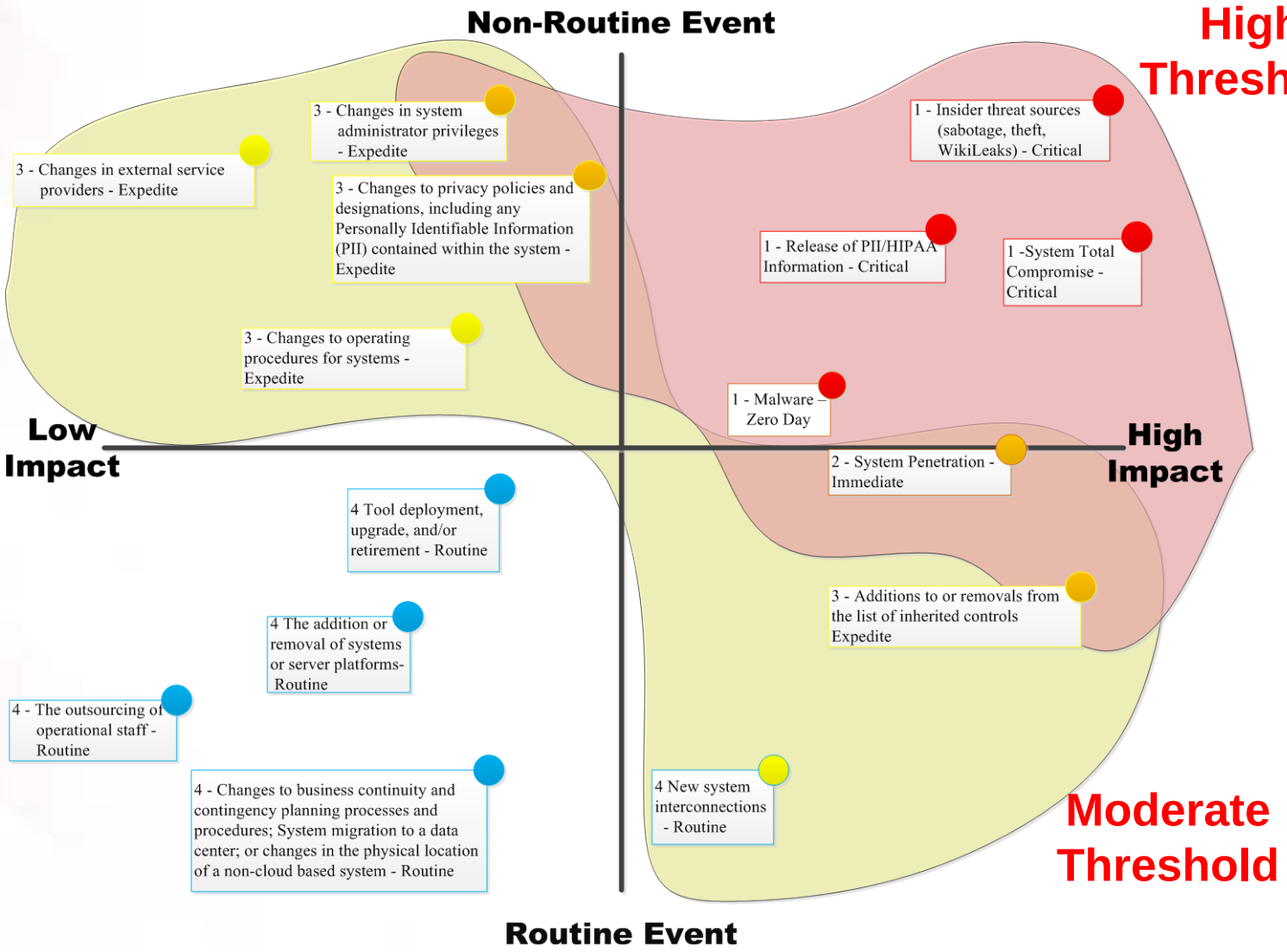
- Existing assessment rigor adequate?
- Identify risk action options
- Escalate visibility (CISO, AO) as appropriate

Examples of Options

- Create a POA&M Action
- Update assessment frequency
- Revisit NIST RMF Steps 1-5

Homeland Security

Defining Risk Threshold



Triggers Evolving

Severity	Description	Risk Threshold
	People	
1	Insider threat sources (e.g. sabotage, theft)	High
3	Changes in external service providers	High
3	Changes in system administrator privileges	High
4	The outsourcing of operational staff	Low
	Processes	
2	Malware	Mod
2	System Penetration	Mod
3	Changes to operating procedures for systems	High
3	Changes to privacy policies and designations	High
3	**Changes to organizational missions/business functions and associated mission/business processes/applications***	High
3	**Changes in data/information types (added or removed) to be processed or stored on the system which could potentially trigger adjustment to information and information system categorization and/or security control adjustments.***	High
4	Updates to federal policies and guidelines	Low
4	Changes to business continuity and contingency planning processes	Low
	Technology	
1	Total System Compromise	High
1	Release of PII Information	High
2	Malware	Mod
2	System Penetration	Mod
3	Additions to or removals from the list of inherited security controls	High
4	Tool deployment, upgrade, and/or retirement	Low
4	**Enterprise architecture changes (including the upgrade, addition or removal of information systems or system components)***	Low
4	Operating System (OS) changes	Low
4	New system interconnections	Low
4	Changes to physical facility, e.g., HVAC, power	Low

Homeland Security

*** Blue Text = NIST Input**

Triggers Exercised by Components

- Three months of pilot data

Component	# of Active Systems	Trigger Risk Threshold			Total
		High	Moderate	Low	
ICE	6	1	6	8	**15**
TSA	2	0	6	9	**15**
DHS HQ	1	0	4	1	**5**
USCIS	0	0	0	0	**0**
TOTALS	**9**	**1**	**16**	**18**	**35**

Moderate Example

Continuous Monitoring Scan Triggers Potential Concern

OA Manager Informed and notifies ORMB members; ORMB Meeting Scheduled

ORMB Actions:
- **Correct configuration issues**
- **Recently migrated to monthly (frequency) continuous monitoring scorecard**
- **Notify CISO**
- **Notify AO (routine weekly)**

Control: AC-6/CM-6

Weakness: Least Privilege/ Configuration Settings

Severity: 2

Description: Based on the DP Protect Scans on the System-1 Database, multiple improper access controls and permissions (Guest, Public) accounts:

- High - Permission on registry extended procedures (2 instances)
- Medium - Permissions granted to GUEST (50 instances)
- Medium - Permissions granted to PUBLIC (2659 instances)
- Medium - Unauthorized object permission grants (30 instances)
- Low - Permission to select from system table (1176 instances)
- Low - Permissions granted to user (3 instances)

Description:	ORMB Meeting
Meeting Date:	Tuesday July 9, 2013
Telephone #:	1-866-000-1234 x9876543#
Time:	11:00 AM – 12:00 PM
OA Manager:	Susan B. Anthony
Scribe:	Ernest Hemingway

Meeting Participants (35)

Name	Group
Benjamin Franklin	CISO (ORMB Chair)
James Madison	System Administrator
Susan B. Anthony	OA Manager
Theodore Roosevelt	ORMB – SA&RM
Robert F. Kennedy	ISSO
…	…

Topic 1:	Introduction
Discussion:	Agenda: o Introductions o Action Items from 7/2/13 ORMB (see below Action Items chart) o System-1 o System-2

Meeting Outputs/Action Items

Item	Actions
System-1: AC-6 /CM-6	• Control Assessment Required/Frequency Updated • Risk Action: Remediate • System-1 Database improper access controls and permissions (Guest, Public) accounts corrected: • High - Permission on registry extended procedures (2 instances CORRECTED) • Medium - Permissions granted to GUEST (50 instances CORRECTED) • Medium - Permissions granted to PUBLIC (2659 instances CORRECTED) • Medium - Unauthorized object permission grants (30 instances CORRECTED) • Low - Permission to select from system table (1176 instances CORRECTED) • Low - Permissions granted to user (3 instances CORRECTED) • AO briefed on status of trigger during weekly OA Update Meeting (TRAL)

Low Example

POA&M Process Triggers Potential Concern

OA Manager Notified

OA Manager recommends System Owner and ISSO submit waiver due to vendor delays in releasing patch

Control: CA-5

Weakness: Overdue POA&M

Severity: 4

Description: POA&M is currently twenty-five (25) days overdue.

No escalation required to ORMB based on the Risk Threshold Matrix (considering the severity of the trigger and the FIPS Categorization of the system)

Action Items

Item	Actions
System-3: CA-5	• Waiver is to be submitted immediately with a Low risk Categorization and referenced in POA&M Tracking Tool • AO briefed on status of trigger during weekly OA Update Meeting (TRAL)

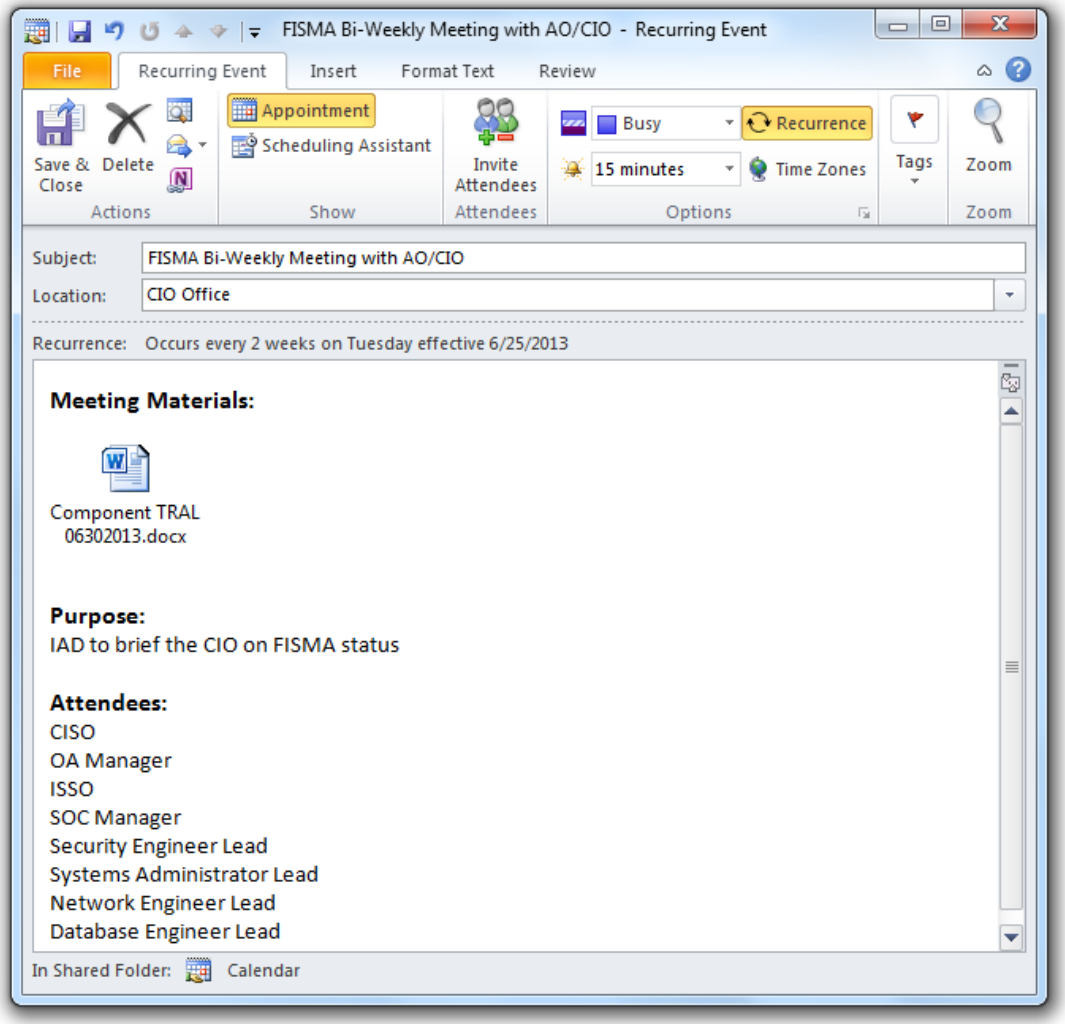
TRigger Accountability Log (TRAL)

Trigger ID	Observed Date	Resolution Date	System Name	Description	Category	Severity	Impacted Controls	Risk Treshold	Risk Action
CMP-00015	6/24/13	6/30/13	SYS-1	In monthly scans, only 9 of 11 system assets reported anti-virus data. Worked with scanning team to rescan assets and confirmed the remaining 2 assets were compliant.	Technology	2	SI-3	Moderate	Mitigation POA&M #5 completed.
CMP-00016	8/1/13	Ongoing	SYS-2	There is a planned migration from Oracle 10g to 11g that will affect the system. Preparations are being made to ensure a seamless, secure transition.	Technology	4	CM-2, SI-2	Low	Accepted - No further action (aside from existing preparations); CISO was notified.
CMP-00018	8/4/13	Ongoing	SYS-2	The monthly Nessus scan identified that 9 Windows servers had outdated patches. Scan results were reviewed to determine criticality and priority of patches. Patching now in progress.	Technology	2	SI-2	Moderate	Mitigation POA&M #6 in process.

All unresolved triggers are forwarded to the POA&M Team within 30 days

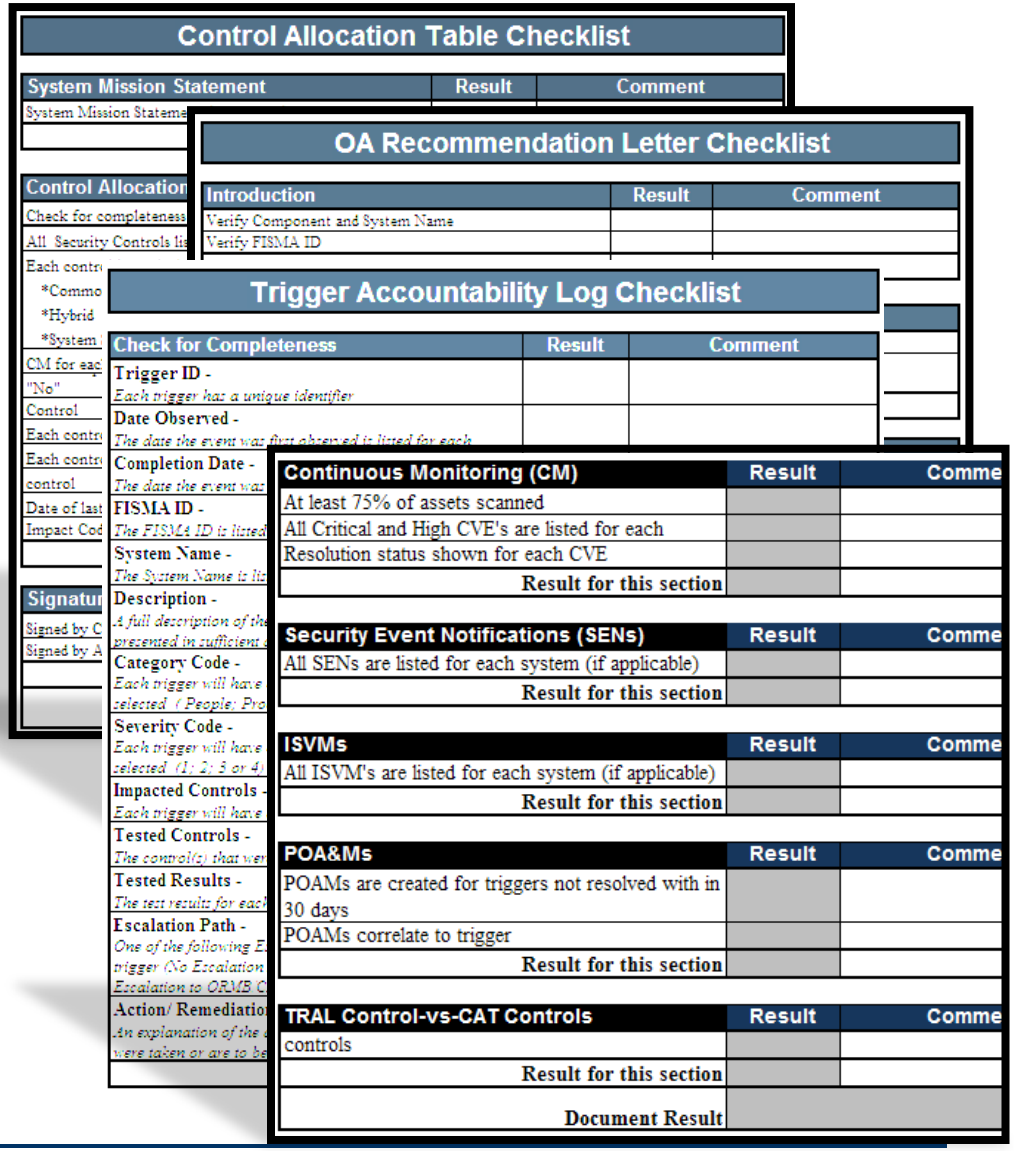
Authorizing Official Involvement

- Only successful if AO maintains an awareness of ongoing risk versus every three years
- DHS Minimum: AO must be made aware of ongoing operational risk at least quarterly. *Reality – Pilot groups reported weekly*
- The majority of triggers may never require AO intervention



OA Quality Assurance

- DHS reviews **OA Artifacts** for completeness and quality against the **DHS OA Quality Assurance Checklist**
- For the pilot, DHS is reviewing nearly all documents to ensure the process is working
- For operational use, DHS would sample results to ensure the proper implementation of the process



Next Steps

- Formal Report of Pilot Results
  - Implement any necessary Policy/Guidance changes

- Continue migrating DHS Systems in Ongoing Authorization

Component Examples

ICE Example of Control Assessment Frequency

This is an example of the assessment frequency based on Control and FIPS Rating. This was generated by ICE SyStats tool (Automated Frequency Generation Tool):

System Type	OA Start Date	Control No	Max Assess Freq Days	First Assess Due Date (randomized first date)	Next Assess Due Date
High (HHH)	8/5/2013	AC-01	730 (2 years)	3/16/2014	3/15/2016
Moderate (MMM)	8/5/2013	AC-01	1095 (3 years)	4/14/2015	4/13/2018
Low (LLL)	8/5/2013	AC-01	1460 (4 years)	5/13/2017	5/12/2021
High (HHH)	8/5/2013	AC-02	365 (1 year)	11/2/2013	11/2/2014
Moderate (MMM)	8/5/2013	AC-02	730 (2 years)	9/27/2014	9/26/2016
Low (LLL)	8/5/2013	AC-02	1095 (3 years)	6/30/2014	6/29/2017
High (HHH)	8/5/2013	AC-03	365 (1 year)	11/21/2013	11/21/2014
Moderate (MMM)	8/5/2013	AC-03	730 (2 years)	10/10/2014	10/9/2016
Low (LLL)	8/5/2013	AC-03	1095 (3 years)	10/4/2014	10/3/2017
High (HHH)	8/5/2013	CA-03	365 (1 year)	2/15/2014	2/15/2015
Moderate (MMM)	8/5/2013	CA-03	730 (2 years)	7/13/2014	7/12/2016
Low (LLL)	8/5/2013	CA-03	1095 (3 years)	5/17/2014	5/16/2017
High (HHH)	8/5/2013	IA-08	730 (2 years)	1/14/2015	1/13/2017
Moderate (MMM)	8/5/2013	IA-08	1095 (3 years)	4/1/2016	4/1/2019
Low (LLL)	8/5/2013	IA-08	1460 (4 years)	11/8/2013	11/7/2017
High (HHH)	8/5/2013	MA-02	730 (2 years)	2/14/2015	2/13/2017
Moderate (MMM)	8/5/2013	MA-02	1095 (3 years)	8/2/2014	8/1/2017
Low (LLL)	8/5/2013	MA-02	1460 (4 years)	1/23/2015	1/22/2019
High (HHH)	8/5/2013	SI-02	182 (6 months)	12/9/2013	6/9/2014
Moderate (MMM)	8/5/2013	SI-02	365 (1 year)	1/29/2014	1/29/2015
Low (LLL)	8/5/2013	SI-02	730 (2 years)	1/10/2014	1/10/2016

Low Volatility

High Volatility

Note: Control assessment due dates are automatically re-baselined if an assessment occurs (due to an Event) earlier than the Maximum Assessment Frequency Days schedule.

TSA OA Experience & Lessons Learned

Requirements

- Systems enter OA Pilot after the ATO has been signed.
- Systems had to have been reporting consistently and accurately with DHS Metric Scorecard data since October 2012 (Patch management, configuration management, vulnerability management, weakness management, ISVMs, ISSO training attendance, Privileged user account records and training, etc.).
- ISSOs must be reliable and engaged.
- CAT tailored to each system, however all contain controls monitored monthly that map to the scorecard metrics.

Systems in Pilot

- MML (Major App), HHH (GSS), pending signatures - HHH (Major App); All are Mission Essential Systems.
- GSSs will be brought in (one is in the pilot at H/H/H) before MAs they host to ensure infrastructure is being monitored monthly for the “core” scorecard controls (CM, SI, AU control families).

Challenges

- Manual process, automation in near future; new scanning schedules for Major Apps and databases; training ISSOs, System Owners, Assessors, Security Engineers, SOC Personnel, Technical SMEs and members of the RMB.

Homeland Security