Boundary Consolidation Case Study

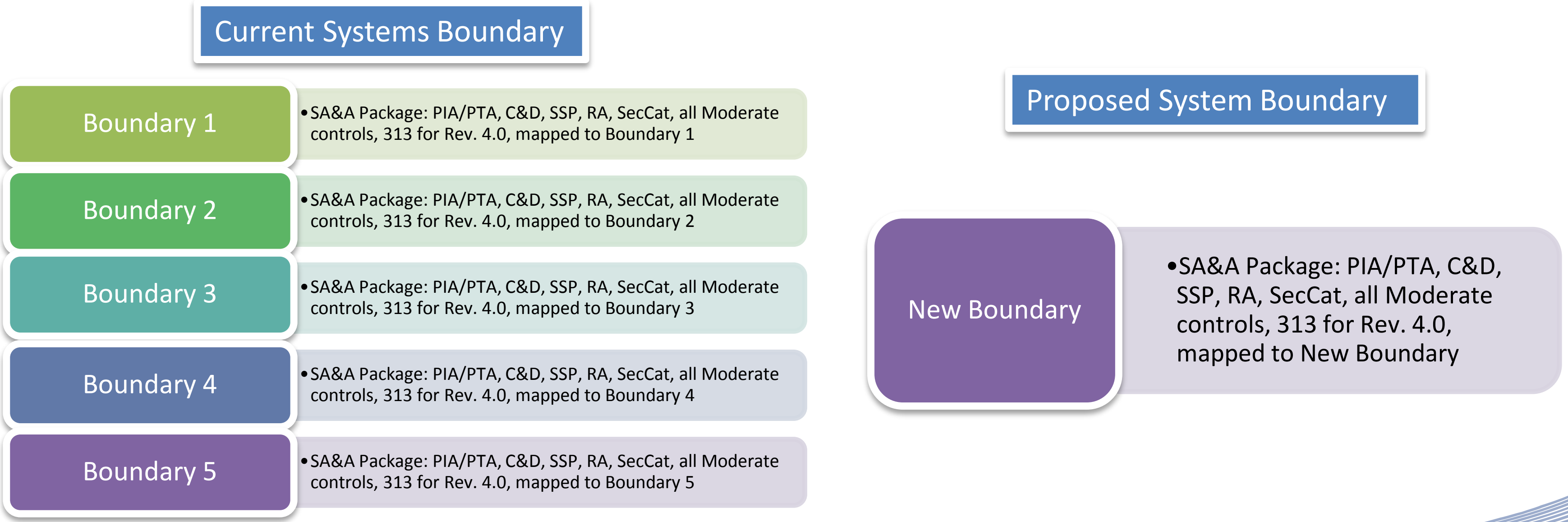
LaCountiss Hopkins, Information System Owner
Baan Alsinawi, OBA Information System Security Officer

Agenda

- Boundary Consolidation
- Why We Did It: Alignment & Efficiencies
- How We did it: Planning, Tailoring of Controls & Overlays
- Results: Control Assessment & Risk Management

Boundary Consolidation

In March 2015, a Business Impact Analysis (BIA) was submitted to the AO, proposing to manage several previously defined FISMA systems into one consolidated boundary. The BIA proposal was the result of an department wide Gap Analysis project, that started in May of 2014 and concluded in January 2015. The boundary recommendation was in alignment with NIST and the overall Gap Analysis Recommendations. The new system boundary provides alignment with department strategic goals, efficiency in level of effort and required resources, as well as overall risk management objectives.



Current Systems Boundary

Boundary 1

- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to Boundary 1

Boundary 2

- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to Boundary 2

Boundary 3

- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to Boundary 3

Boundary 4

- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to Boundary 4

Boundary 5

- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to Boundary 5

Proposed System Boundary

New Boundary

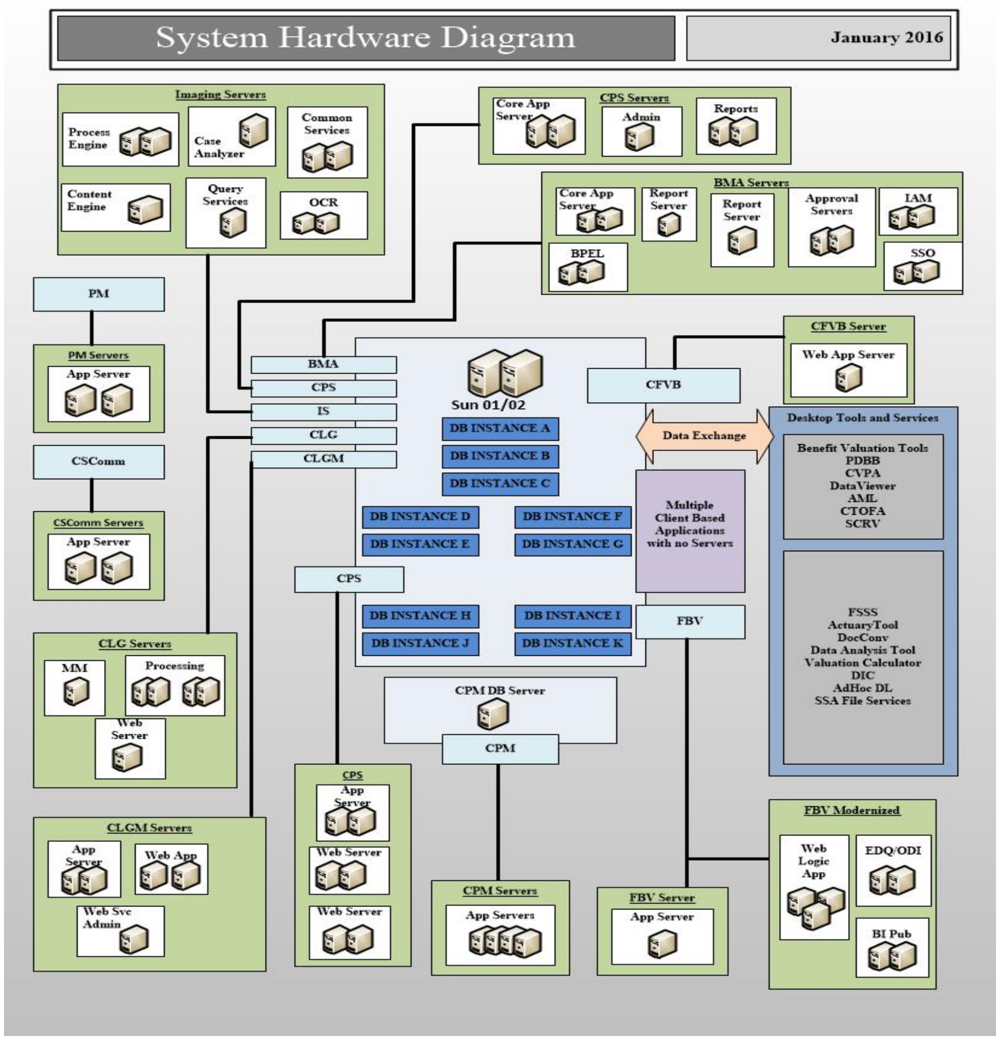
- SA&A Package: PIA/PTA, C&D, SSP, RA, SecCat, all Moderate controls, 313 for Rev. 4.0, mapped to New Boundary

Why We Did It: Alignment

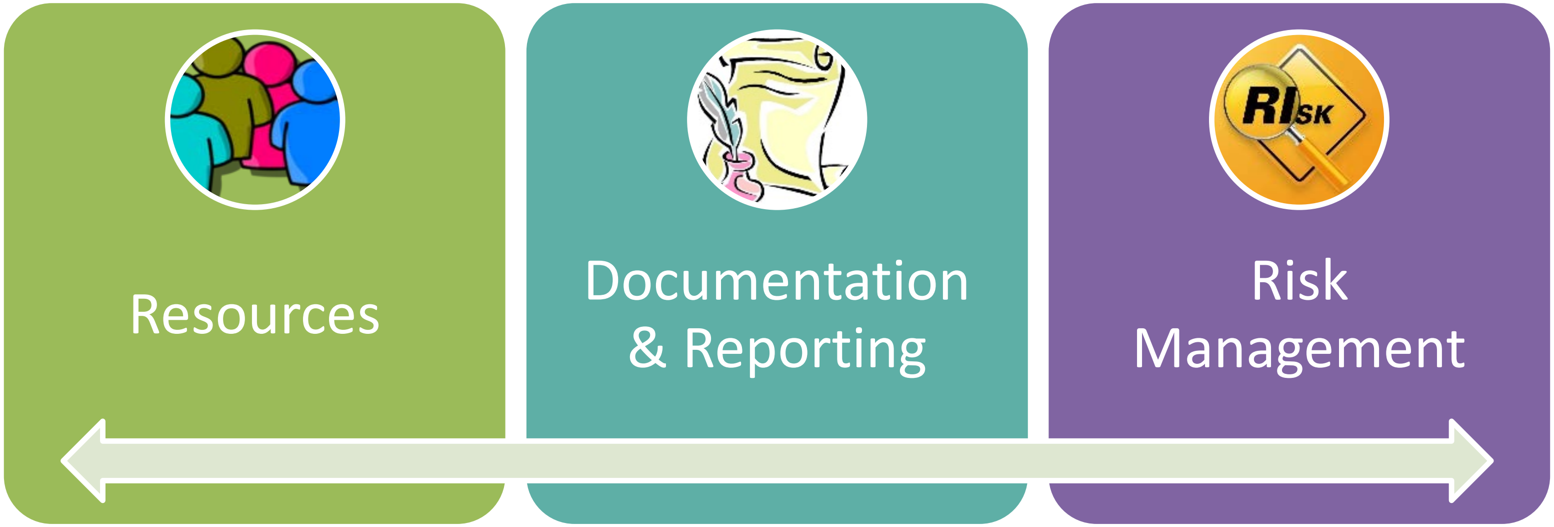
The new boundary consists of multiple applications that facilitate the overall department mission of supporting management of benefit plans and providing benefit services.

The new boundary is classified into 3 major components:

- Server Applications,
- Client Applications, and
- Desktop Tools and Services.



Why We did it: Efficiencies



Resources

Documentation & Reporting

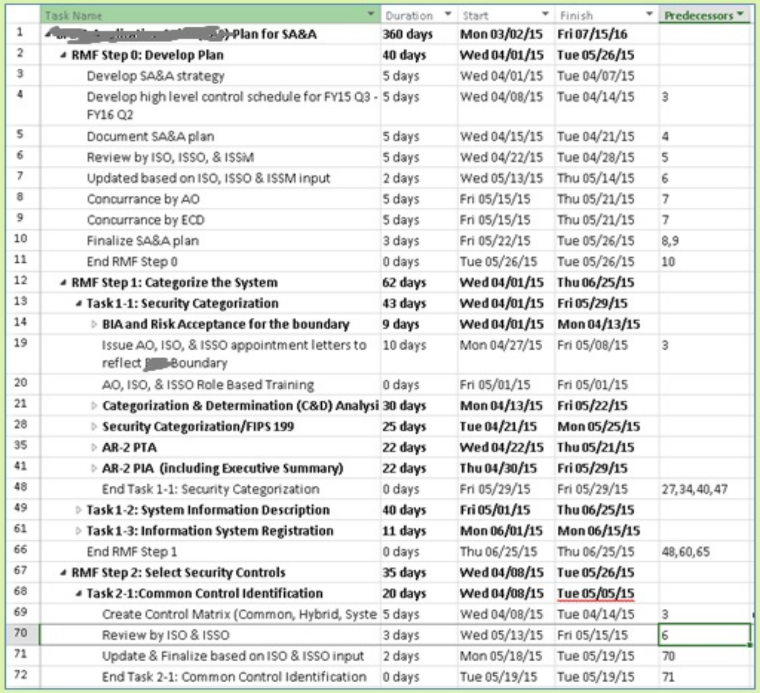
Risk Management

- Multiple resources from different operational units assigned security responsibilities part-time as part of “other duties as assigned”
- Resource allocations were not based on risk or system complexity.

- Documentation processes, standards, and quality varied widely across the different systems
- Management communications were inconsistent in content and frequency

- Cohesive understand of security compliance and risks was not available
- Quantification and oversight of risks were lacking.

How We Did It: Planning



	Task Name	Duration	Start	Finish	Predecessors
1	**[redacted] Plan for SA&A**	**360 days**	**Mon 03/02/15**	**Fri 07/15/16**	
2	**RMF Step 0: Develop Plan**	**40 days**	**Wed 04/01/15**	**Tue 05/26/15**	
3	Develop SA&A strategy	5 days	Wed 04/01/15	Tue 04/07/15	
4	Develop high level control schedule for FY15 Q3 - FY16 Q2	5 days	Wed 04/08/15	Tue 04/14/15	3
5	Document SA&A plan	5 days	Wed 04/15/15	Tue 04/21/15	4
6	Review by ISO, ISSO, & ISSM	5 days	Wed 04/22/15	Tue 04/28/15	5
7	Updated based on ISO, ISSO & ISSM input	2 days	Wed 05/13/15	Thu 05/14/15	6
8	Concurrance by AO	5 days	Fri 05/15/15	Thu 05/21/15	7
9	Concurrance by ECD	5 days	Fri 05/15/15	Thu 05/21/15	7
10	Finalize SA&A plan	3 days	Fri 05/22/15	Tue 05/26/15	8,9
11	End RMF Step 0	0 days	Tue 05/26/15	Tue 05/26/15	10
12	**RMF Step 1: Categorize the System**	**62 days**	**Wed 04/01/15**	**Thu 06/25/15**	
13	**Task 1-1: Security Categorization**	**43 days**	**Wed 04/01/15**	**Fri 05/29/15**	
14	**BIA and Risk Acceptance for the boundary**	**9 days**	**Wed 04/01/15**	**Mon 04/13/15**	
19	Issue AO, ISO, & ISSO appointment letters to reflect [redacted] Boundary	10 days	Mon 04/27/15	Fri 05/08/15	3
20	AO, ISO, & ISSO Role Based Training	0 days	Fri 05/01/15	Fri 05/01/15	
21	**Categorization & Determination (C&D) Analysi**	**30 days**	**Mon 04/13/15**	**Fri 05/22/15**	
28	**Security Categorization/FIPS 199**	**25 days**	**Tue 04/21/15**	**Mon 05/25/15**	
35	**AR-2 PTA**	**22 days**	**Wed 04/22/15**	**Thu 05/21/15**	
41	**AR-2 PIA (including Executive Summary)**	**22 days**	**Thu 04/30/15**	**Fri 05/29/15**	
48	End Task 1-1: Security Categorization	0 days	Fri 05/29/15	Fri 05/29/15	27,34,40,47
49	**Task 1-2: System Information Description**	**40 days**	**Fri 05/01/15**	**Thu 06/25/15**	
61	**Task 1-3: Information System Registration**	**11 days**	**Mon 06/01/15**	**Mon 06/15/15**	
66	End RMF Step 1	0 days	Thu 06/25/15	Thu 06/25/15	48,60,65
67	**RMF Step 2: Select Security Controls**	**35 days**	**Wed 04/08/15**	**Tue 05/26/15**	
68	**Task 2-1:Common Control Identification**	**20 days**	**Wed 04/08/15**	**Tue 05/05/15**	
69	Create Control Matrix (Common, Hybrid, Syste	5 days	Wed 04/08/15	Tue 04/14/15	3
70	Review by ISO & ISSO	3 days	Wed 05/13/15	Fri 05/15/15	6
71	Update & Finalize based on ISO & ISSO input	2 days	Mon 05/18/15	Tue 05/19/15	70
72	End Task 2-1: Common Control Identification	0 days	Tue 05/19/15	Tue 05/19/15	71

Project plan served as the road map.

- NIST RMF was basis for project plan
  - Each RMF Step was delineated to capture all the tasks necessary to complete activities and associated deliverables associated
- Planned the Plan
  - Over a month of planning was dedicated to RMF Step 0: Develop the Plan
- Socialized plan to ensured support
  - Enterprise Cyber-Security Division (ECD)
  - Privacy Office
  - Department Directors
- Obtained approval from AO & CISO to ensure commitment

How We Did It: Tailored Controls & Overlays

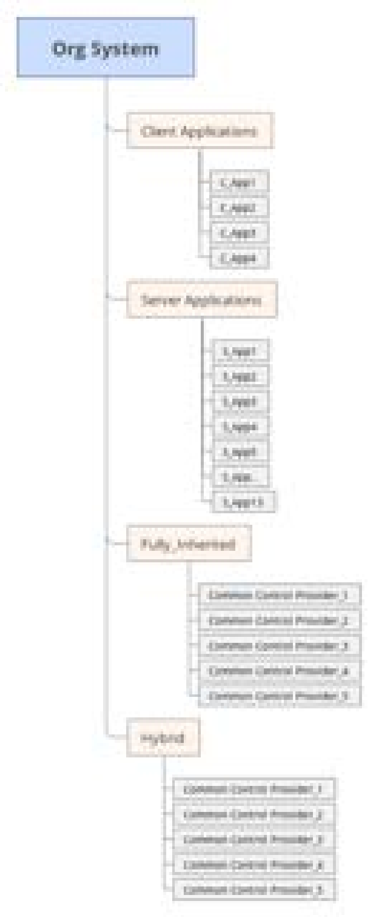
NIST 800-37 Rev 1.0 emphasizes the benefits of *controls tailoring*, where tailoring provides flexibility in applying the risk management concepts associated with the RMF in a manner that is most suitable for the organizations and the information systems involved.

The controls, and later assessment of risk and mapping of applicable POA&M items, were scoped according to:

- System Specific
- Hybrid_Inherited
- Fully_Inherited

By applying the Moderate Baseline for NIST 800-53 Rev 4.0 of 313 controls, and scoping some controls to be assessed at the Client Application level and/or the Server application level, the OBA security process had the following advantages:

- Leveraging efficiencies from CCP and avoiding the duplication of efforts
- Assessing risk at the appropriate level within the system boundary
- Overall improved resource allocation and risk management processes

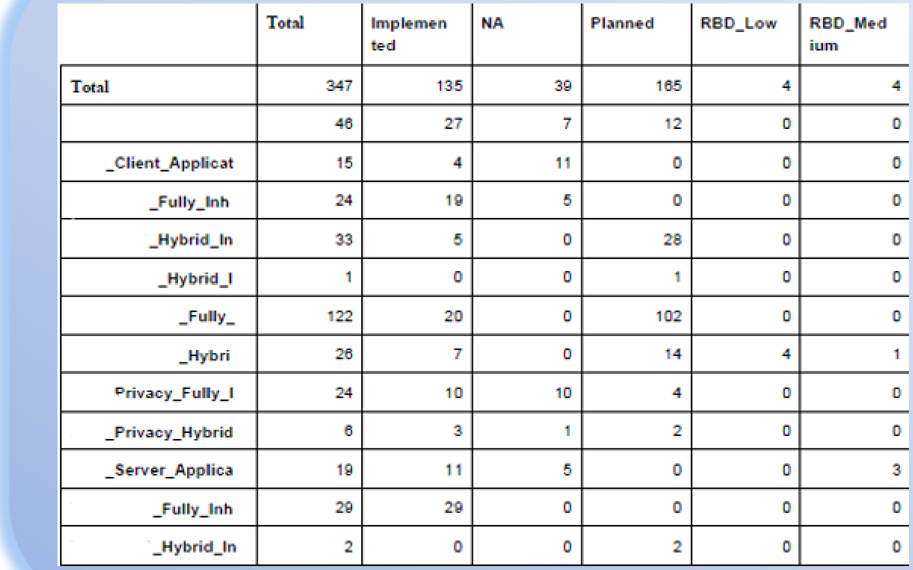

Org System
Client Applications
C_App1
C_App2
C_App3
C_App4
Server Applications
S_App1
S_App2
S_App3
S_App4
S_App5
S_App...
S_App13
Fully_Inherited
Common Control Provider_1
Common Control Provider_2
Common Control Provider_3
Common Control Provider_4
Common Control Provider_5
Hybrid
Common Control Provider_1
Common Control Provider_2
Common Control Provider_3
Common Control Provider_4
Common Control Provider_5

Results: Controls Analysis

In accordance with the NIST 800-53A and the control tailoring used for the new boundary, a total of 396 controls were analyzed throughout the SAA process from April 2015 through March 2016.

Some details on the process:

- There was a total of 347 controls System wide but some were assessed more than once, either repeated in multiple quarters or assessed for multiple categories such as Client, Server or Inherited.
- While the team did not perform an analysis of the Fully Inherited controls, the ISCM process did include an assessment of risks inherited as a result of a weakness in any of the Common Control Providers programs.
- The team analyzed and assessed the system specific component of all Hybrid controls.



	Total	Implemented	NA	Planned	RBD_Low	RBD_Medium
Total	347	135	39	165	4	4
	46	27	7	12	0	0
_Client_Applicat	15	4	11	0	0	0
_Fully_Inh	24	19	5	0	0	0
_Hybrid_In	33	5	0	28	0	0
_Hybrid_I	1	0	0	1	0	0
Fully	122	20	0	102	0	0
_Hybri	26	7	0	14	4	1
Privacy_Fully_I	24	10	10	4	0	0
_Privacy_Hybrid	6	3	1	2	0	0
_Server_Applica	19	11	5	0	0	3
_Fully_Inh	29	29	0	0	0	0
_Hybrid_In	2	0	0	2	0	0

Results: Risk Management

Plan of Action & Milestones (POAMs)

After the initial defining and consolidation of the boundary architecture and components, a total of **42 POA&Ms** identifying risk areas that were system specific or inherited according to the controls tailoring were tracked throughout the ISCM process.

On an ongoing basis, the OBA team in collaboration with the ECD, IT, and the Privacy Offices were able to close most of the POA&M's.

At the end of the SAA assessment only **1 POA&M remain**.

A detailed Risk Assessment and Business Impact Analysis process was followed throughout the SA&A process, presenting the AO with the necessary information to make risk based decisions related to the boundary's system security.

In instances where identified weaknesses could not be remediated within an acceptable time frame according to the OBA POA&M process, the ISCM team followed the BIA and Risk Acceptance processes.

A total of 28 Risk Based Decisions were tracked during the assessment period, 12 of those remain at the end of the process.

Risk Acceptances (RA)

Results: FY2015-2016 Improvements

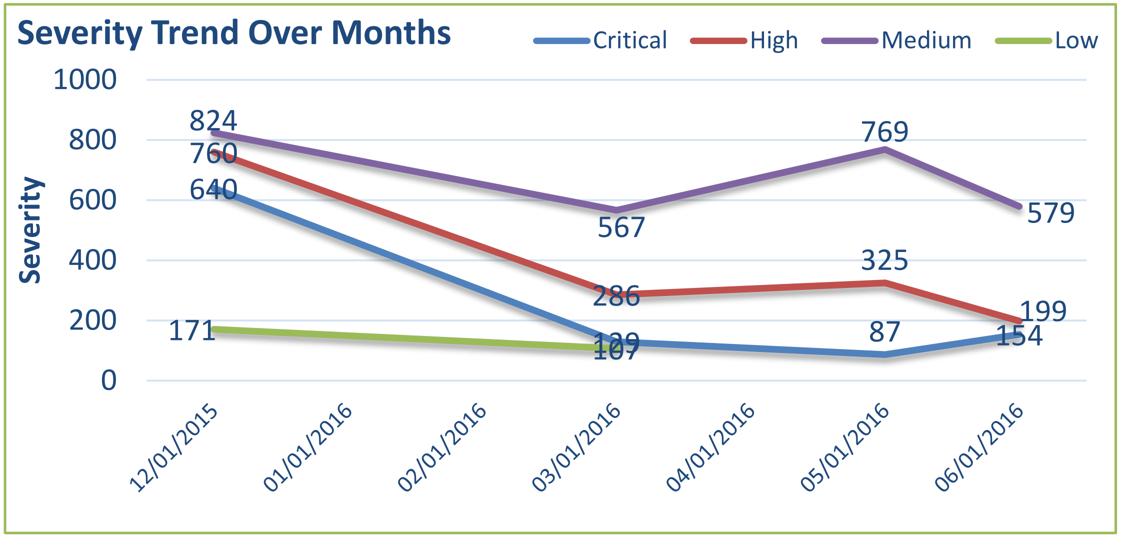
The SA&A process was performed along with a number of process improvement initiatives and projects, some at the Security Program Level and some at the enterprise levels, a few listed below:

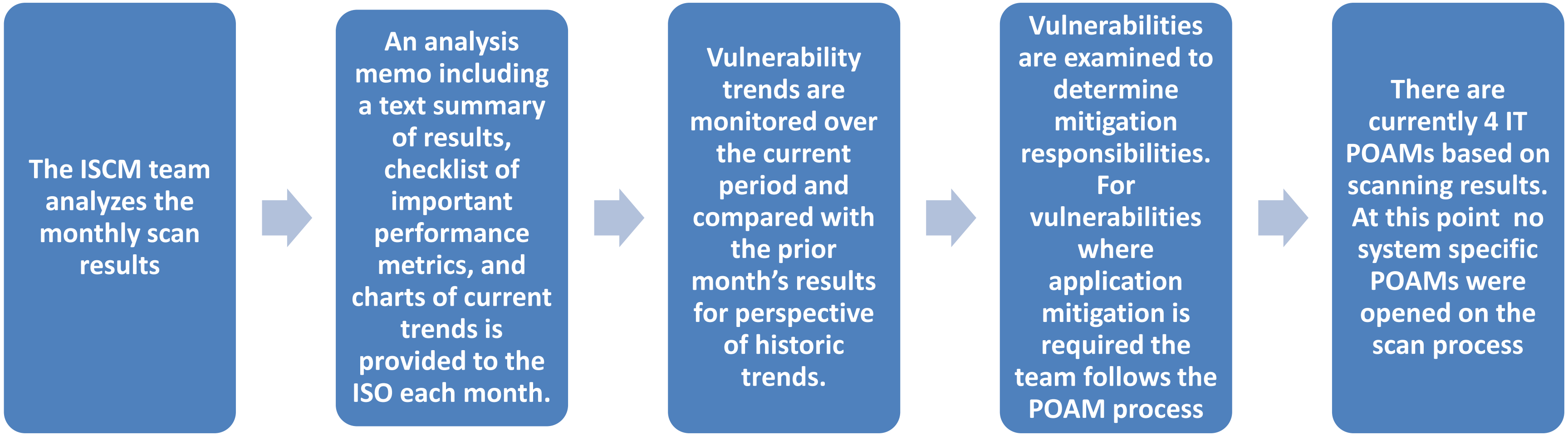
- Identified Orphan Systems that were added to the new boundary based on risk analysis
- Established a compliance and configuration management process using IBM Endpoint Manager (IEM) in collaboration with IT
- Leveraged enterprise implementation of an audit logging tool to coordinate and capture audit logs created by applications
- Ensured all components are assessed based on NIST 800-53 Rev 4.0 controls
- Addressed Organizationally Defined Parameters and Common Controls in collaboration with ECD
- In tandem with the ongoing assessment of the boundary components, the Security team worked with development teams on modernizing their systems, adding to the boundary as these systems moved from development into production
- Supported enterprise wide efforts and the ongoing change management and integrated process teams

Results: Vulnerability Management

Further details on another process improvement is the OBA vulnerability management process as seen below.

The process was established to allow for tracking of vulnerabilities over time and trend analysis.





The ISCM team analyzes the monthly scan results

An analysis memo including a text summary of results, checklist of important performance metrics, and charts of current trends is provided to the ISO each month.

Vulnerability trends are monitored over the current period and compared with the prior month's results for perspective of historic trends.

Vulnerabilities are examined to determine mitigation responsibilities. For vulnerabilities where application mitigation is required the team follows the POAM process

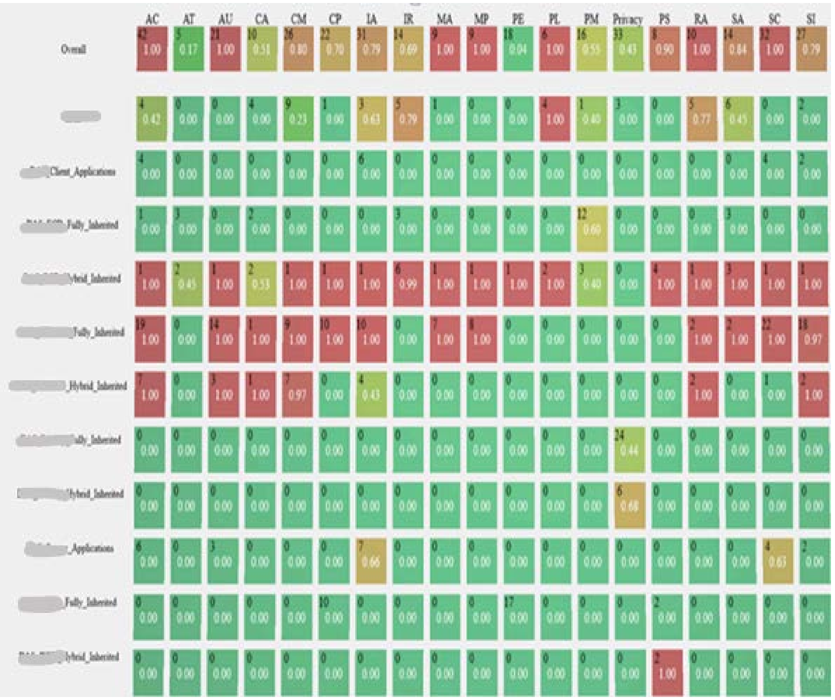
There are currently 4 IT POAMs based on scanning results. At this point no system specific POAMs were opened on the scan process

Results: Managing Risk Using Metrics

Facilitated the definition of a security baseline for the boundary introducing risk metrics as proposed by the NIST publications are shown here. The goal of the ISCM process is to minimize the residual risk exposure of the boundary.

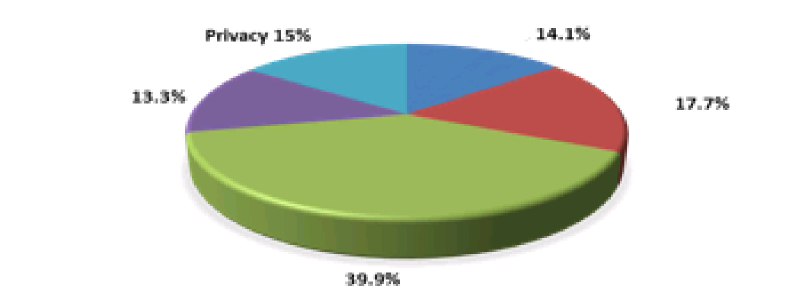
The inclusion of risk metrics provides the OBA security with the following:

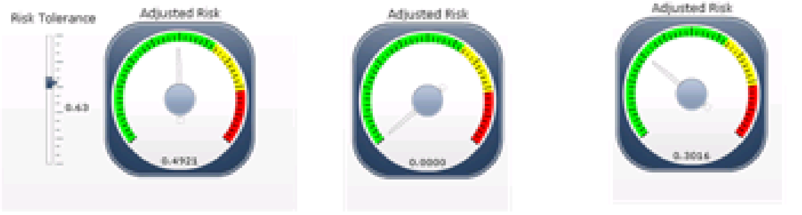
- ✓ Access to quantifiable measures used for evaluating the ISCM process for measures of success or lack thereof over time
- ✓ Ability to establish a baseline for risk tolerance based on the overall remaining residual risk values after all reasonable efforts are made to manage risks effectively
- ✓ Metrics that can be used to determine the overall effect of security methods implemented within the program



	AC	AT	AU	CA	CM	CP	IA	IR	MA	MP	PE	PL	PM	Privacy	PS	RA	SA	SC	SI
Overall	42 1.00	5 0.17	21 1.00	10 0.51	26 0.80	22 0.70	31 0.79	14 0.69	9 1.00	9 1.00	18 0.04	6 1.00	16 0.55	33 0.43	8 0.90	10 1.00	14 0.84	32 1.00	27 0.79
[redacted]	4 0.42	0 0.00	0 0.00	4 0.00	9 0.23	1 0.00	3 0.63	5 0.79	1 0.00	0 0.00	0 0.00	4 1.00	1 0.40	3 0.00	0 0.00	5 0.77	6 0.45	0 0.00	2 0.00
[redacted]Client_Applications	4 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	6 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	4 0.00	2 0.00
[redacted]Fully_Inherited	1 0.00	3 0.00	0 0.00	2 0.00	0 0.00	0 0.00	0 0.00	3 0.00	0 0.00	0 0.00	0 0.00	0 0.00	12 0.60	0 0.00	0 0.00	0 0.00	3 0.00	0 0.00	0 0.00
[redacted]ybrid_Inherited	1 1.00	2 0.45	1 1.00	2 0.53	1 1.00	1 1.00	1 1.00	6 0.99	1 1.00	1 1.00	1 1.00	2 1.00	3 0.40	0 0.00	4 1.00	1 1.00	3 1.00	1 1.00	1 1.00
[redacted]Fully_Inherited	19 1.00	0 0.00	14 1.00	1 1.00	9 1.00	10 1.00	10 1.00	0 0.00	7 1.00	8 1.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	2 1.00	2 1.00	22 1.00	18 0.97
[redacted]_Hybrid_Inherited	7 1.00	0 0.00	3 1.00	1 1.00	7 0.97	0 0.00	4 0.43	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	2 1.00	0 0.00	1 0.00	2 1.00
[redacted]ully_Inherited	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	24 0.44	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00
[redacted]ybrid_Inherited	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	6 0.68	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00
[redacted]_Applications	6 0.00	0 0.00	3 0.00	0 0.00	0 0.00	0 0.00	7 0.66	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	4 0.63	2 0.00
[redacted]Fully_Inherited	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	10 0.00	0 0.00	0 0.00	0 0.00	0 0.00	17 0.00	0 0.00	0 0.00	0 0.00	2 0.00	0 0.00	0 0.00	0 0.00	0 0.00
[redacted]ybrid_Inherited	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	0 0.00	2 1.00	0 0.00	0 0.00	0 0.00	0 0.00

SYSTEM SPECIFIC AND INHERITED RISKS

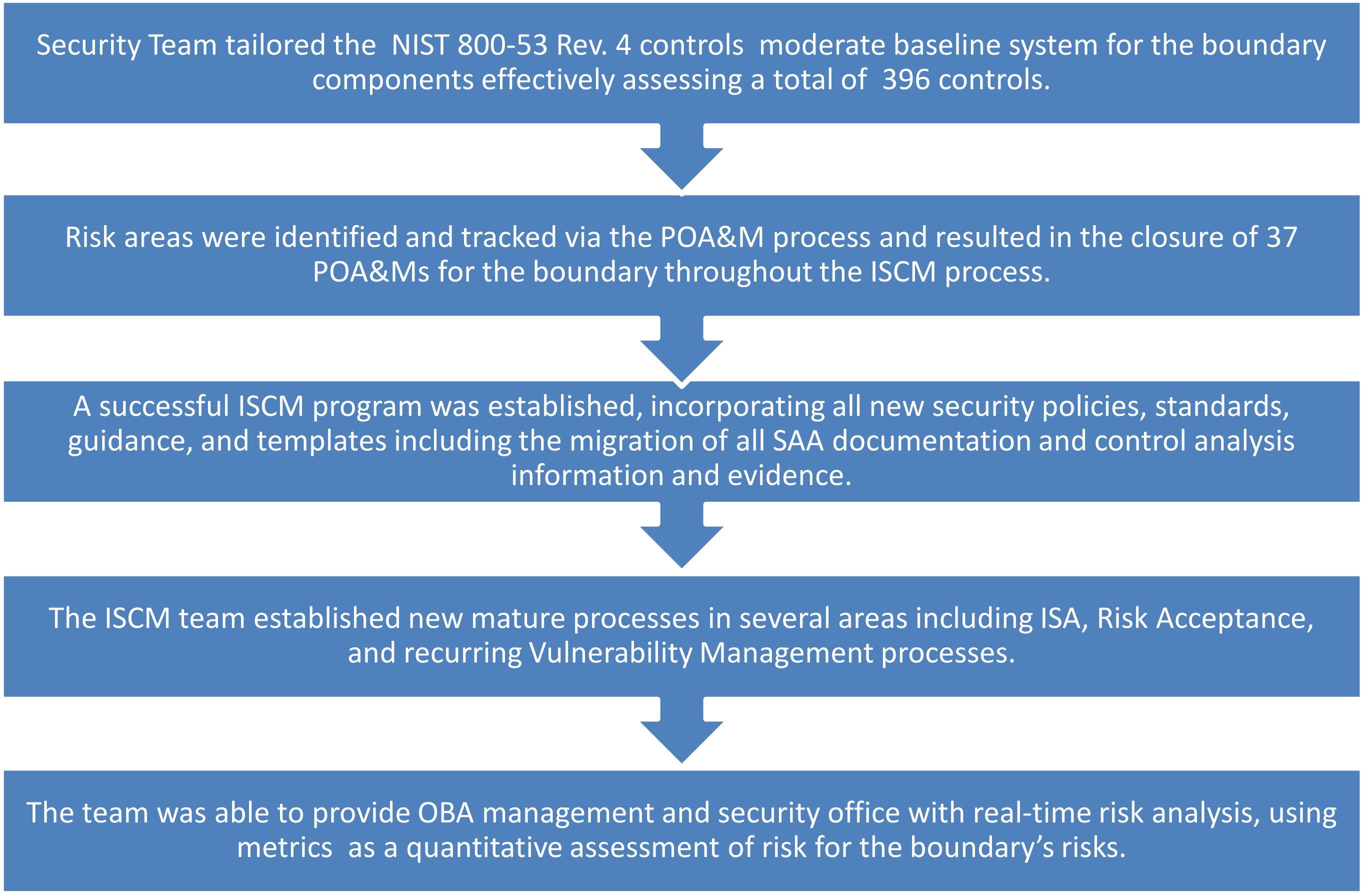




0.49 (Moderate)	Client Applications 0.00 (Moderate)	Server Applications 0.30 (Moderate)

Consolidation Summary

During the Q3 FY2015 - Q2 FY2016 assessment period, the SA&A process successfully implemented the risk management framework and yielded the following results:



Security Team tailored the NIST 800-53 Rev. 4 controls moderate baseline system for the boundary components effectively assessing a total of 396 controls.

Risk areas were identified and tracked via the POA&M process and resulted in the closure of 37 POA&Ms for the boundary throughout the ISCM process.

A successful ISCM program was established, incorporating all new security policies, standards, guidance, and templates including the migration of all SAA documentation and control analysis information and evidence.

The ISCM team established new mature processes in several areas including ISA, Risk Acceptance, and recurring Vulnerability Management processes.

The team was able to provide OBA management and security office with real-time risk analysis, using metrics as a quantitative assessment of risk for the boundary's risks.

Questions?