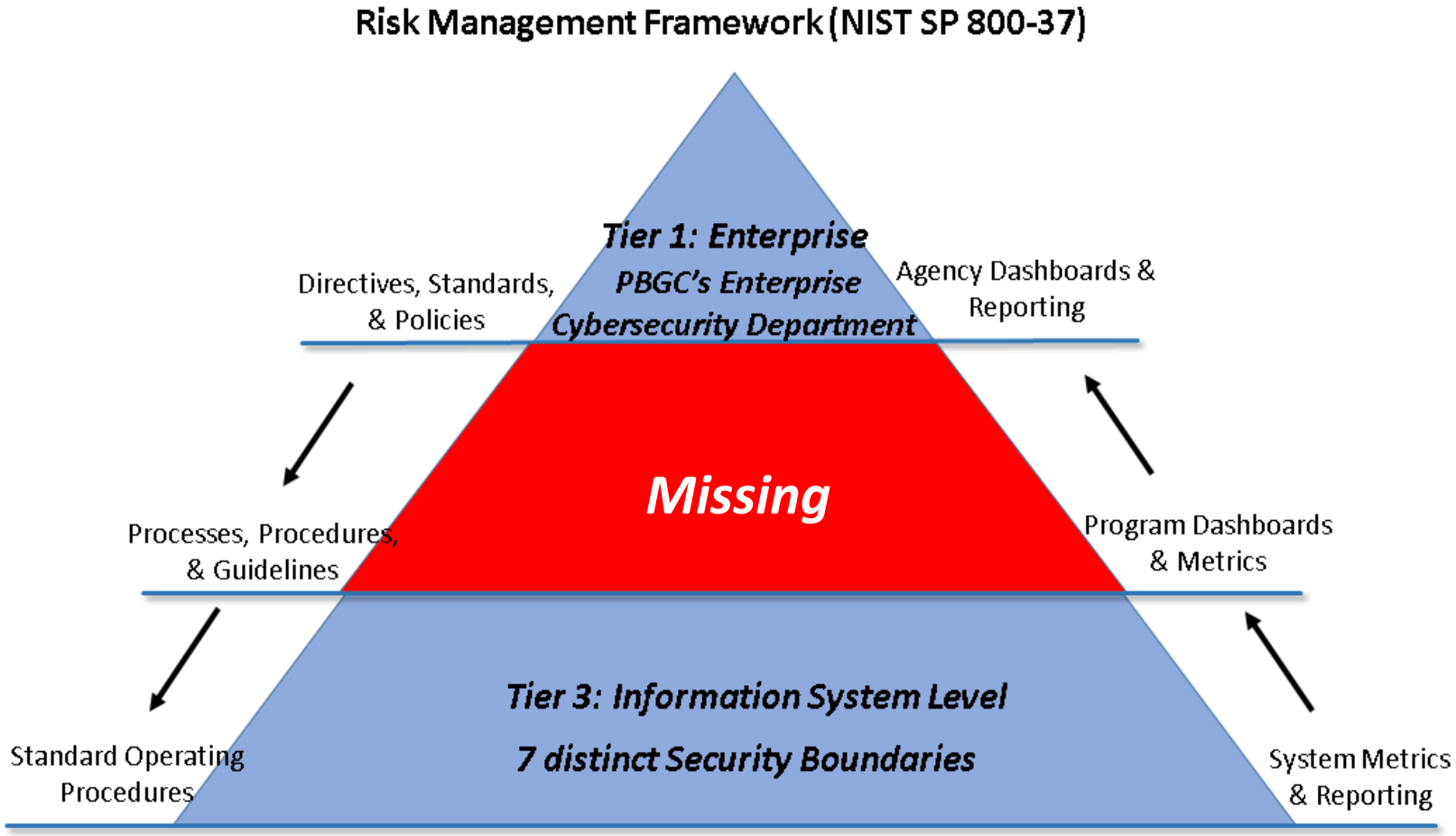
Department wide Gap Analysis & Establishing a Tier 2 Information Security Risk Management Program

Debra Graul, Information System Security Manager
Taryne McDonald, Information Owner

Outline

- Rationale
- Fundamentals of Gap Analysis
  - Standards, Metrics, & Project Management
- Results
  - Findings & Recommendations
- Implementation
  - Current State & Future Plans
- Conclusion

Rationale


Risk Management Framework (NIST SP 800-37)
Tier 1: Enterprise
PBGC's Enterprise Cybersecurity Department
Directives, Standards, & Policies
Agency Dashboards & Reporting
Missing
Processes, Procedures, & Guidelines
Program Dashboards & Metrics
Tier 3: Information System Level
7 distinct Security Boundaries
Standard Operating Procedures
System Metrics & Reporting

Foundation for Gap Analysis

Gap Analysis: Standards

NIST

- **NIST SP 800-30**: Guide for Conducting Risk Assessments
- **NIST SP 800-37**: Risk Management Framework
- **NIST SP 800-53**: Security & Privacy Controls for Federal Information Systems & Organizations
- **NIST IR 7358:** Program Review of Information Security Management Assistance (PRISMA)

ISACA Risk IT Framework

- **Governance, Risk Management & Compliance Framework**
- **Align** the management of business risk with agency & department tolerances
- **Balance** costs & benefits of managing risk , based on business impact assessments
- **Promote** fair & open communication of risk between all stakeholders
- **Establish** a continuous process that is part of daily activities

Gap Analysis: Standards

Key Practice Areas (KPAs) identify core area of information systems security risk management for this analysis. The attributes serve as a indicator of the effectiveness of the systems for that practice area. KPAs and attributes provide context and consistent evaluation of the system's security and risk management.

Key Practice Area 1 - Information Security Deliverables

- 1.1 Completeness
- 1.2 Quality/Accuracy

Key Practice Area 2 - Resources Core Competencies

- 2.1 Education, Training and Experience
- 2.2 Security Knowledge & Technical Expertise

Key Practice Area 3 - Processes, Procedures & Standard

- 3.1 Controls Review & Assessment
- 3.2 Adherence to Risk Management

Gap Analysis: Metrics

Metrics allow for:

- Quantifiable measures for the KPAs using defined attributes
- Objective review of the Risk Management Standards
- Baselining current state of risk across all security boundaries
- Ability to set goals for a department wide risk management & continuous monitoring program

Category	Description
Initial	Emergent understanding that IT risk is important and needs to be managed.
Defined	IT risk management is viewed as a business issue, and both downside and upside of IT risk are recognized.
Managed	IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood.
Optimized	Senior executives make a point of considering all aspects of IT risk in their decisions.

Gap Analysis: Metrics

Metric	KPA 1.1 – Completeness Attribute Measured Criteria
1	The risks are not identified in the deliverable. The controls are not mapped against the risk appropriately. Does not provide sufficient narrative in describing risk aspects of the system in relation to the deliverable's objective. Does not provide sufficient supporting evidence for determinations of system related risks.
2	The risks are not completely identified in the deliverable. Most of the controls are mapped against the risk appropriately. Does not provide sufficient narrative in describing risk aspects of the system in relation to the deliverable's objective. Does not provide sufficient supporting evidence for determinations of system related risks.
3	The risks are somewhat identified in the deliverable. The controls are mapped against the risk appropriately. Information Security deliverable provides some narrative in describing risk aspects of the system in relation to the deliverable's objective. Does not provide sufficient supporting evidence for determinations of system related risks.
4	The risks are completely identified in the deliverable. The controls are mapped against the risk appropriately. Information Security deliverable provides sufficient narrative in describing risk aspects of the system in relation to the deliverable's objective. Information Security deliverable provide sufficient supporting evidence for determinations of system related risks.

KPA 1.1 – Completeness Attribute

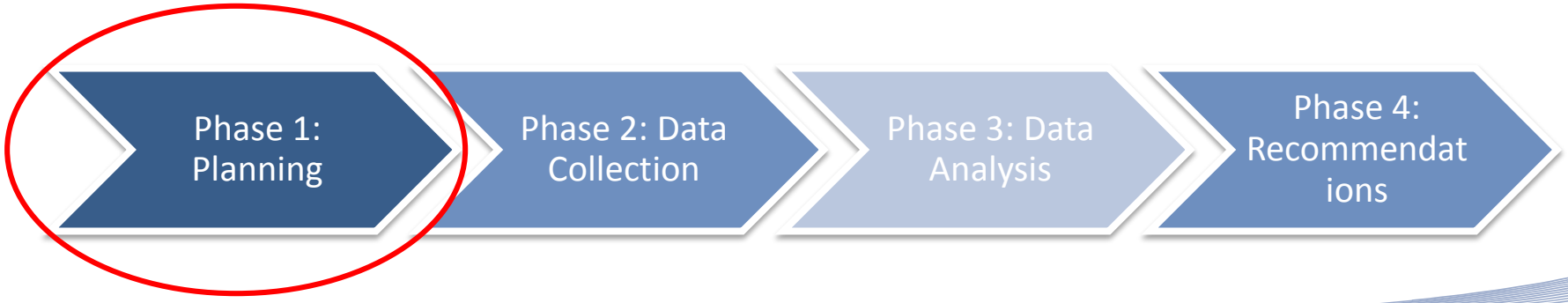
Completeness of Information Security Deliverables – It is always recommended the overall system narrative for any system be complete and consistent, ensure description of risk areas in the proper level of detail (boundary, data sensitivity, applied controls etc.).

To determine the completeness the entire set of deliverables are reviewed individually & comparatively against each other to:

- ✓ Ensure risks are consistently reviewed with supporting evidence and cited rationale for determination of risk
- ✓ The details are complete including comprehensive references to NIST controls and standards in the risk narrative
- ✓ Ensure that the system security documents are reviewed on an defined basis via continuous monitoring

Gap Analysis: Project Management

- ✓ Stakeholder Interviews
- ✓ Scope, Goal, Objectives
- ✓ Project Planning Document
- ✓ Communications Plan
- ✓ Project Schedule
- ✓ Project Charter
- ✓ Kick-off Meetings
- ✓ System & Program Assessment Results



Gap Analysis: Project Management

- ✓ Communications with ISO / IO / CORs was key early in project to ensure clarify scope, set expectations, & to gain buy-in of their support
- ✓ Early delivery of references to security team helped avoid surprises & allowed for sufficient responses on their part

Security Documentation List

#	Document Title/Description	NIST Control Family	Required
1	Information System Risk Assessment	RA, CA	Yes
2	System Security Plan (SSP) & SSP Workbook	CA, (All NIST Controls)	Yes
3	Privacy Threshold Assessment (PTA)/Privacy Impact Assessment (PIA)	PC, SC	Yes
4	Seccat Document	CA, RA	Yes
5	ATO Documents	CA	Yes
6	All Risk Acceptances (if not included in SSP)	Applicable	Yes
7	Memorandum of Understanding (MOU) and/or Interconnection Security Agreement (ISA)	CA, AC, PL, SC & SC	Yes
8	Detailed system/network architecture diagram with IP addresses of devices that will be in scope (if not included in SSP)	SC, AC, CM PM	Yes
9	Latest POA&M Report Submitted to the ECD	CA, PL, RA	Yes
10	Latest Account Recertification Documents	AC, PS, PL	
11	Rules of Behavior (If Applicable)	AC, PL, PS	
12	Contingency Plans	CP, CM, IR	
13	Any NFR Responses to CCRD	CA, RA	
14	Information Security Continuous Monitoring Plan (ISCMP)	CA, PL, PM	

Security Control List

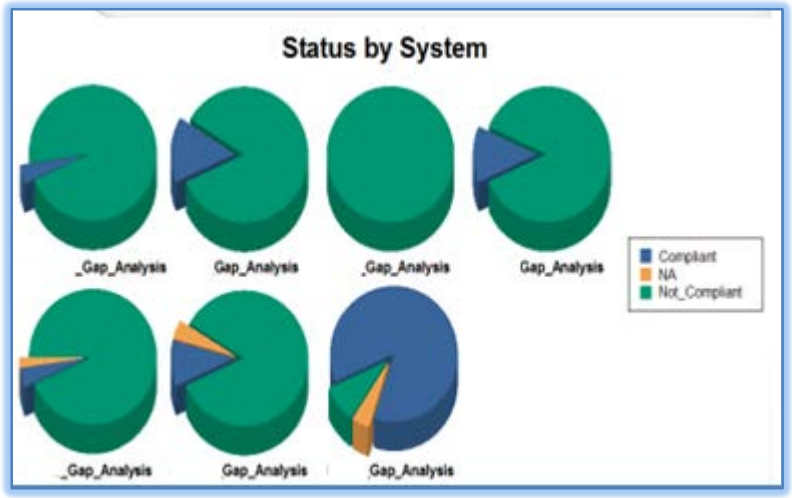
Sampling NIST Control/Enhancement
Access Control
Audit and Accountability
Security Assessment and Authorization
Configuration Management
Contingency Planning
Identification and Authentication
Incident Response
Physical and Environmental Protection
Planning
Program Management
Risk Assessment
System and Services Acquisition
System and Communications Protection
System and Information Integrity

Interview Questionnaire

Results: Metrics

Residual Risk Metrics

Control Compliance Results

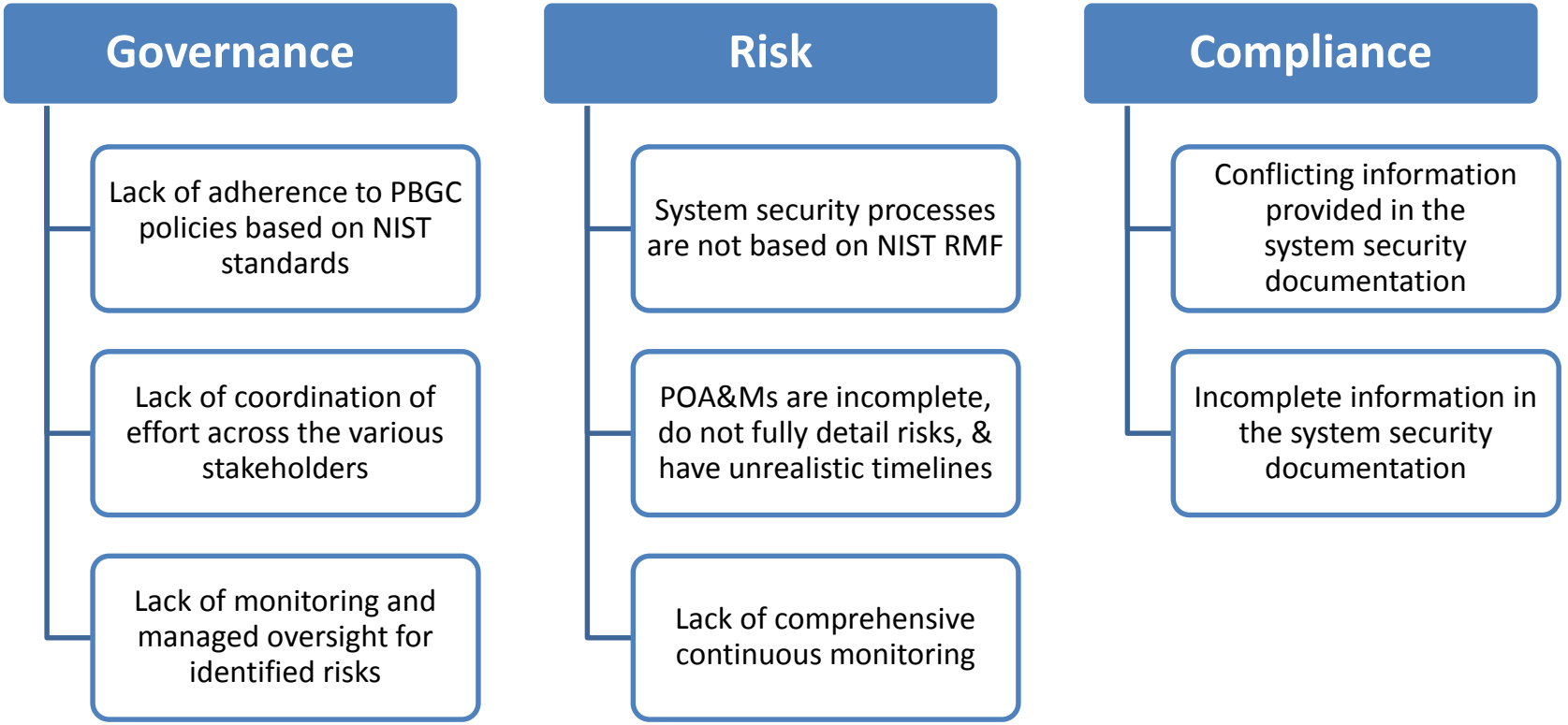


Key Performance Area Measurements

KPA 1.1: Completeness	KPA 1.2: Quality	KPA 2.1 Education, Training & Certification	KPA 2.2 Experience & Proficiency	KPA 2.3: Security Knowledge & Technical Expertise	KPA 3.1 Controls Review & Assessment	KPA 3.2: Adherence to NIST standards
Initial	Initial	Initial	Initial	Initial	Initial	Initial
Defined	Defined	Defined	Defined	Defined	Defined	Defined
Managed	Managed	Managed	Managed	Managed	Managed	Managed
Optimized	Optimized	Optimized	Optimized	Optimized	Optimized	Optimized

Results: Findings

8 findings common across most of the boundaries were tied to the GRC framework



Results: Recommendations

Establish an **Information Security Strategic Plan** focused on enhancing security across department

Refine **Information Security Structure** & alignment of resources

Ensure true comprehensive **ISCM,** Replacing the point-in-time SA&A process for all systems

Improve **Communications** & enhance consolidated **project management**

Develop a Comprehensive Program **Information Security Architecture**, including defining control mapping for all systems

Implementation: Standards

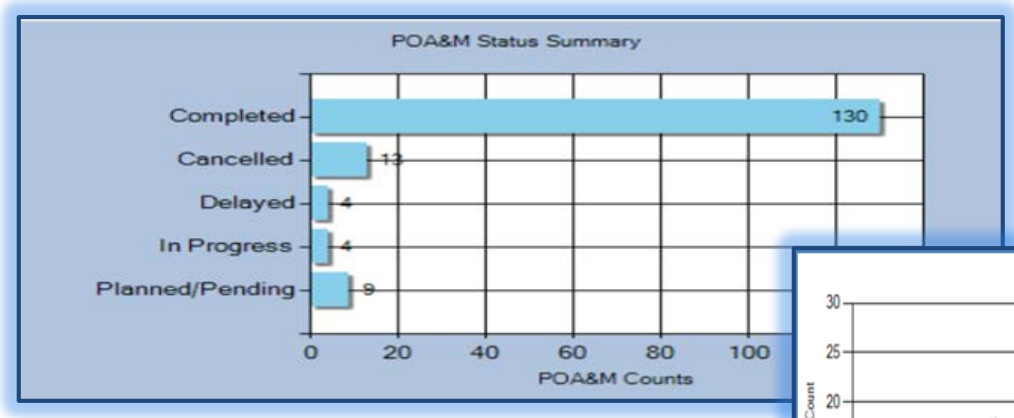
Personnel

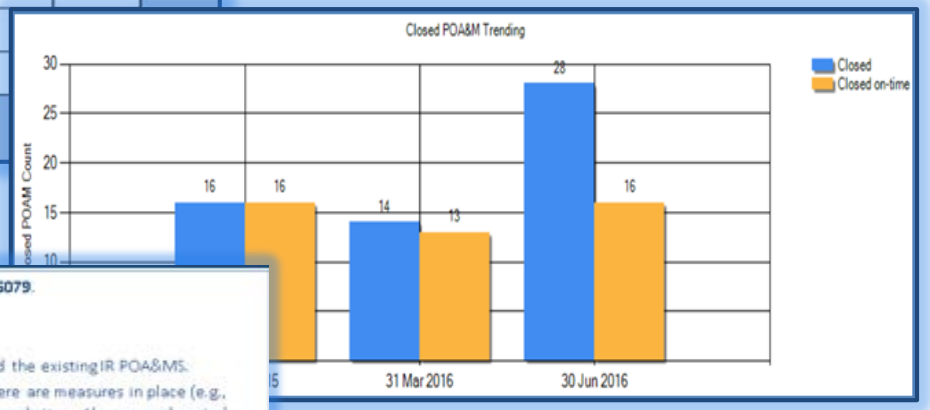
- Staff is all full-time dedicated security professionals
- Added security related measures to performance standards
- Training & Certification requirements

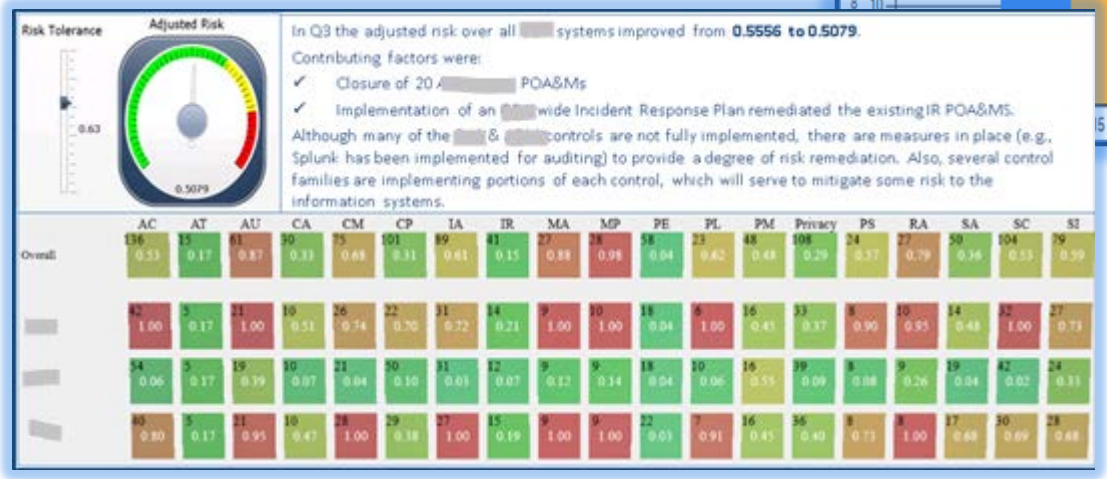
Security & Risk Management

- All systems have achieved on-going authorization status
- All systems have completely full control assessment under 800-53 Rev. 4
- All systems have implemented risk based approach to ISCM planning to ensure alignment of work activities and analysis
- All department risk have been properly documented via business impact assessments, risk acceptances, and POAMs as applicable

Implementation: Metrics







Implementation: Project Management

Information Security Risk Management Program

- Integrated ISSO role into Tier 2 organization
- Defined & appointed ISSM
- Documented roles & responsibilities for security team

Communications

- Schedule & planning for different management reports
- Clarified purpose & scope for various documentation

Processes, Procedures, & templates established

- Created templates & documentation standard for all key deliverables
- ISCM plan based on RMF used by all security teams
- Risk Management process with procedures for: Business Impact Assessment (BIA), Risk Acceptance (RA), & POAM

Implementation: Future

Personnel

- Staff will be placed under GS 2210 series
- All security staff will be professionally certificated by end of FY2017
- Staff realignment due to modernization / decommissioning of systems in FY2018

Program

- Approval of 3 year strategy plan for security program in early FY2017
- Gap analysis on vendor management in FY2017
- Develop a budget forecasting model for security cost in FY2017
- Ongoing maturation of existing security processes & procedures; Development of additional processes & on-line publication starting in FY2017
- Shared business services boundary analysis in FY2018

OBA
OFFICE OF BENEFITS ADMINISTRATION

Questions?