Federal Computer Security Managers' Forum

US Census Bureau
Risk Management Framework

August 27, 2015

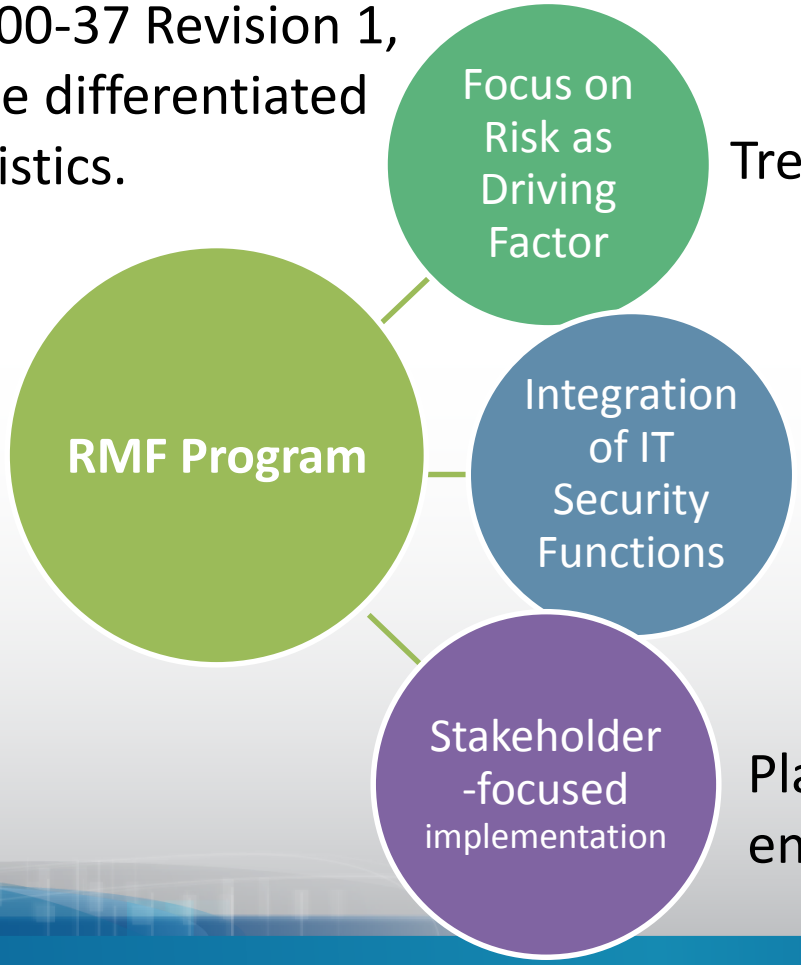
Jaime Lynn Noble

Agenda

- Defining Characteristics of Census Bureau's RMF Program
  - Focus on Risk
  - Integration of IT Security Functions
  - Stakeholder-Focused Implementation
- How We Did It – Risk Reporting and Continuous Monitoring
- RMF Program Accomplishments
- RMF Program Scalability and Future State

Characteristics of Census Bureau's RMF Program

The Census Bureau implemented the RMF Program in accordance with NIST SP 800-37 Revision 1, With three differentiated characteristics.



Treat risk as center of equation

Break down functional silos to achieve program efficiencies

Place emphasis on stakeholders/ end-users

Our Differentiators - Focus on Risk

Risk to the enterprise serves as the core element of our decision making process for cyber actions. Focusing on risk, rather that compliance, allows the bureau to make business-oriented decisions

Application of security controls	Risk Profile Questionnaire to scope and tailor controls based on business and technological factors
Development of risk metrics	Established risk “points” for each control based on potential impact to Confidentiality, Integrity, and Availability and set an agency risk threshold
Increased use of Common Controls and Overlays	Established 3 tiers of Common Control Providers (CCP): Technology-based, Organizational, and Enterprise covering 80% of baseline security controls

Our Differentiators - Integration of IT Security Functions

Correlating previously siloed functions allowed the Bureau to realize cost and process efficiencies in execution across workstreams

Embed **security engineers** in Integrated Project Teams to facilitate security early in the development lifecycle

Incorporate security engineering recommendations in **Risk Profile**

Incorporate results from **automated scanning** and manual security control assessments into single risk report

Our Differentiators - Stakeholder-Focused Implementation

Security **stakeholders** and **senior management** were actively involved in designing the RMF program to create support for change at all levels

RMF Piloting

- Interviewed individuals from system-level staff to senior management to garner feedback on proposed RMF implementation
- Implemented phased, process pilots with targeted business areas and obtained feedback
- Obtained key stakeholder and senior management buy-in

Governance and Training

- Developed and executed detailed Change Management strategy
- Hold bi-monthly Information Security Community forums
- Hold monthly policy working group meetings
- Deliver role-based training
- Deliver content-specific training (e.g. Process, 800-53 Rev 4)

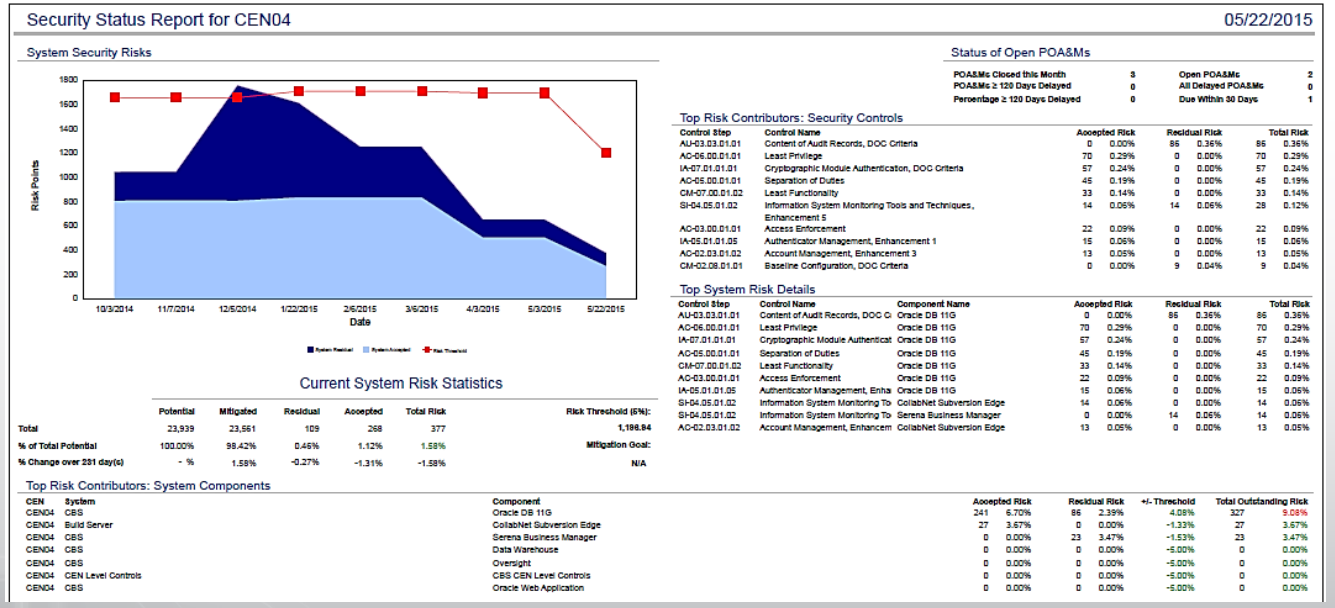
Risk Reporting

- Generate on-going Risk Reports that include results of ISCM assessments
- Detailed assessment results with risk points associated with each control failure
- Risk-based decision-making capabilities (e.g. spending, remediation prioritization)

How We Did It - Risk Reporting

Risk reporting on **assessment status** allows for **On-going Authorization** of systems and gives our stakeholders the tools to understand and manage cyber risk.

- **Trend in overall residual risk**, broken down by inherited risk, accepted risk, and risk to be mitigated by the POA&M
- **System-specific risk analysis**
- **Top risk contributors** by security controls & system component
- **Status of open POA&Ms**



Security Status Report for CEN04 — 05/22/2015

System Security Risks

Status of Open POA&Ms

POA&Ms Closed this Month	3	Open POA&Ms	2
POA&Ms ≥ 120 Days Delayed	0	All Delayed POA&Ms	0
Percentage ≥ 120 Days Delayed	0	Due Within 30 Days	1

Top Risk Contributors: Security Controls

Control Step	Control Name	Accepted Risk		Residual Risk		Total Risk	
AU-03.03.01.01	Content of Audit Records, DOC Criteria	0	0.00%	86	0.36%	86	0.36%
AC-06.00.01.01	Least Privilege	70	0.29%	0	0.00%	70	0.29%
IA-07.01.01.01	Cryptographic Module Authentication, DOC Criteria	57	0.24%	0	0.00%	57	0.24%
AC-05.00.01.01	Separation of Duties	45	0.19%	0	0.00%	45	0.19%
CM-07.00.01.02	Least Functionality	33	0.14%	0	0.00%	33	0.14%
SI-04.05.01.02	Information System Monitoring Tools and Techniques, Enhancement 5	14	0.06%	14	0.06%	28	0.12%
AC-03.00.01.01	Access Enforcement	22	0.09%	0	0.00%	22	0.09%
IA-05.01.01.05	Authenticator Management, Enhancement 1	15	0.06%	0	0.00%	15	0.06%
AC-02.03.01.02	Account Management, Enhancement 3	13	0.05%	0	0.00%	13	0.05%
CM-02.06.01.01	Baseline Configuration, DOC Criteria	0	0.00%	9	0.04%	9	0.04%

Top System Risk Details

Control Step	Control Name	Component Name	Accepted Risk		Residual Risk		Total Risk	
AU-03.03.01.01	Content of Audit Records, DOC C	Oracle DB 11G	0	0.00%	86	0.36%	86	0.36%
AC-06.00.01.01	Least Privilege	Oracle DB 11G	70	0.29%	0	0.00%	70	0.29%
IA-07.01.01.01	Cryptographic Module Authenticat	Oracle DB 11G	57	0.24%	0	0.00%	57	0.24%
AC-05.00.01.01	Separation of Duties	Oracle DB 11G	45	0.19%	0	0.00%	45	0.19%
CM-07.00.01.02	Least Functionality	Oracle DB 11G	33	0.14%	0	0.00%	33	0.14%
AC-03.00.01.01	Access Enforcement	Oracle DB 11G	22	0.09%	0	0.00%	22	0.09%
IA-05.01.01.05	Authenticator Management, Enha	Oracle DB 11G	15	0.06%	0	0.00%	15	0.06%
SI-04.05.01.02	Information System Monitoring To	CollabNet Subversion Edge	14	0.06%	0	0.00%	14	0.06%
SI-04.05.01.02	Information System Monitoring To	Serena Business Manager	0	0.00%	14	0.06%	14	0.06%
AC-02.03.01.02	Account Management, Enhancem	CollabNet Subversion Edge	13	0.05%	0	0.00%	13	0.05%

Current System Risk Statistics

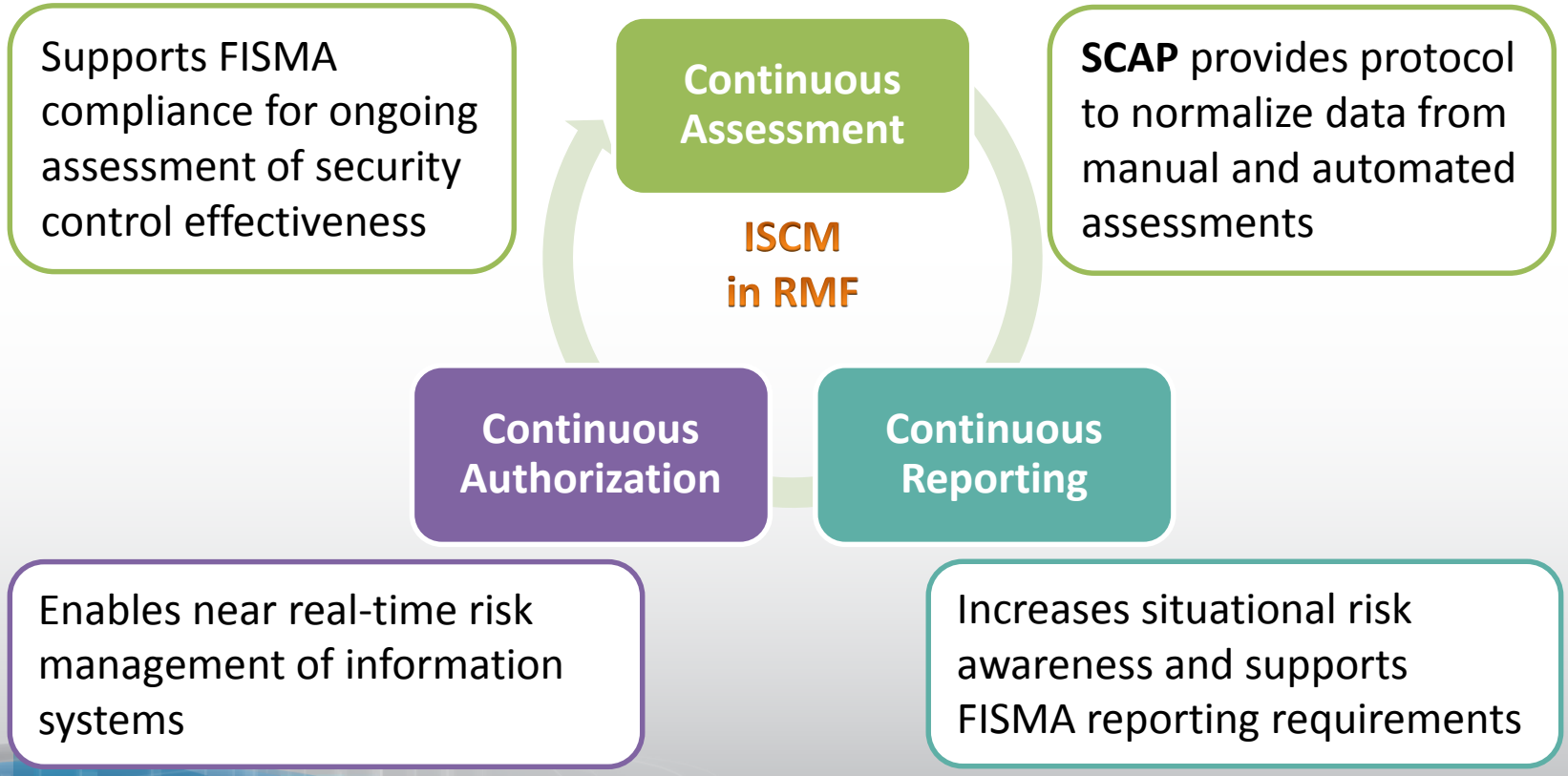
	Potential	Mitigated	Residual	Accepted	Total Risk	
Total	23,939	23,561	109	268	377	Risk Threshold (5%): 1,198.84
% of Total Potential	100.00%	98.42%	0.46%	1.12%	1.58%	Mitigation Goal:
% Change over 231 day(s)	- %	1.58%	-0.27%	-1.31%	-1.58%	N/A

Top Risk Contributors: System Components

CEN	System	Component	Accepted Risk		Residual Risk		+/- Threshold	Total Outstanding Risk	
CEN04	CBS	Oracle DB 11G	241	6.70%	86	2.39%	4.08%	327	9.08%
CEN04	Build Server	CollabNet Subversion Edge	27	3.67%	0	0.00%	-1.33%	27	3.67%
CEN04	CBS	Serena Business Manager	0	0.00%	23	3.47%	-1.53%	23	3.47%
CEN04	CBS	Data Warehouse	0	0.00%	0	0.00%	-5.00%	0	0.00%
CEN04	CBS	Oversight	0	0.00%	0	0.00%	-5.00%	0	0.00%
CEN04	CEN Level Controls	CBS CEN Level Controls	0	0.00%	0	0.00%	-5.00%	0	0.00%
CEN04	CBS	Oracle Web Application	0	0.00%	0	0.00%	-5.00%	0	0.00%

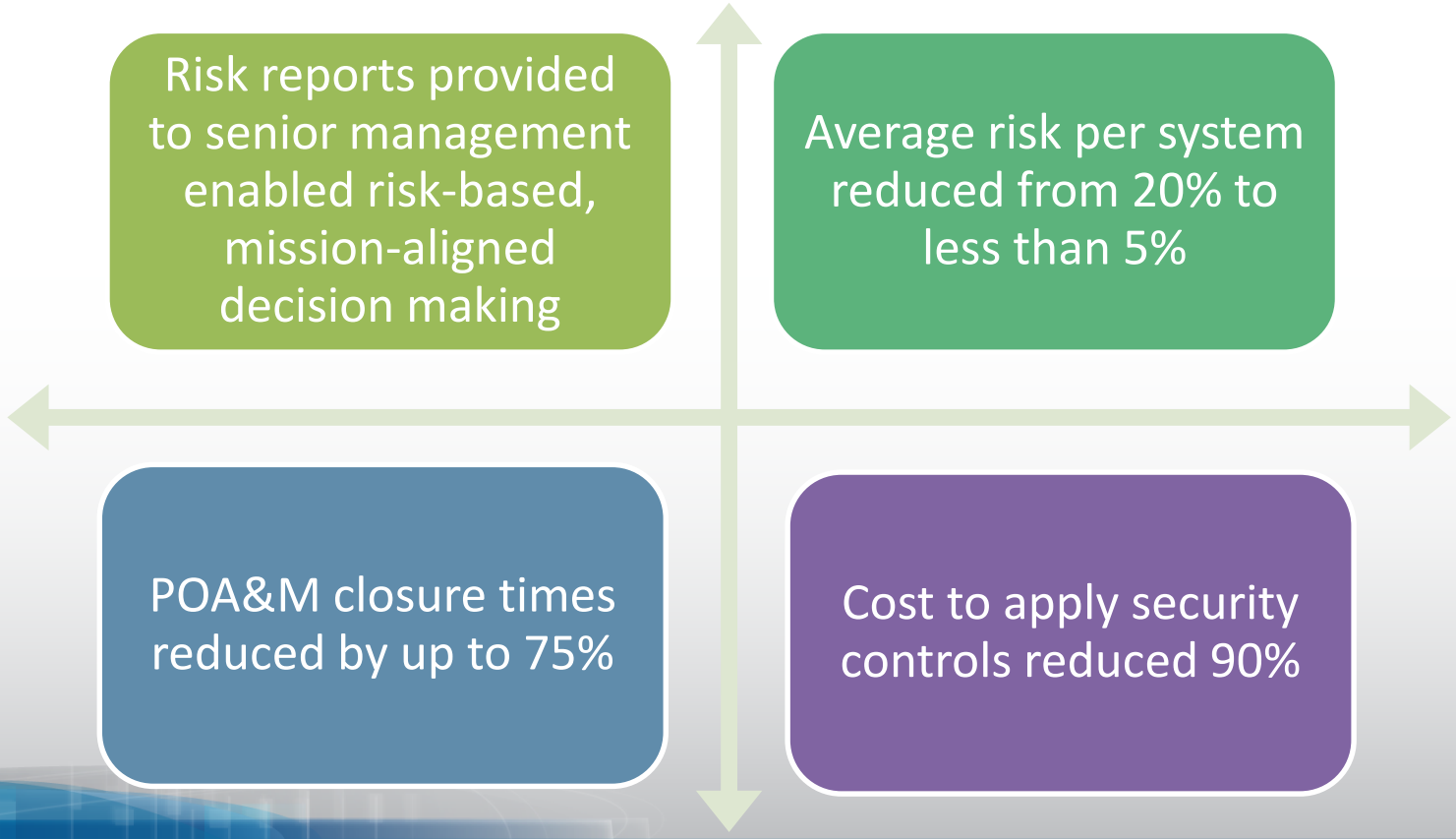
How We Did It - Information System Continuous Monitoring

ISCM consists of **continuous** assessments, reporting, and authorization of information systems to **monitor security risks**



RMF Program Results

Implementation of the RMF Program at the Census Bureau has yielded numerous **qualitative** and **quantitative results**.



Scalability and Next Steps for Our Program

The RMF Program at the Census Bureau was implemented for **scalability**, to address **current** and **future** cybersecurity needs.

- Incorporation of **Federal cyber sprint** objectives, including:

- Next steps: Increased integration of critical security activities, including:

Questions?