Workforce Management in a Continuous Monitoring Paradigm

Jaime Noble, Risk Management Program Manager
US Census Bureau
&
Christian Neeley, Senior Manager
Deloitte & Touche, LLP

United States Census Bureau

Agenda

- Census RMF Program Overview
- Workforce Management in Continuous Monitoring
- Case Study – ISSO's and Specialization of Labor
- Case Study – Authorizing Officials and Risk Management
- Lessons Learned

Program Overview

The US Census Bureau Began its Risk Management Framework (RMF) program transition in 2010, converting the Certification & Accreditation Process into Continuous Monitoring (CM)

- Focused on incorporating risk-based decision making into the authorization process
- Followed the leaders in leveraging automated assessment capabilities
- Incorporated security engineering principles into the early phases of the SDLC

As we moved from pilot phase into the full RMF transition, the need for a coherent and comprehensive approach to understanding and retraining our supporting workforce came clearly into focus.

Workforce Management's Importance in Continuous Monitoring

While Continuous Monitoring is typically characterized by a focus on technology and security, it is the supporting workforce that enables us to transform our approach and deliver enhanced program capabilities

- Major Workforce Themes in CM
  - Security skillsets continue to become more specific, requiring more personnel trained in security engineering and in enterprise risk management
  - Capitalizing on economies of scale allows for specialization of labor and better aligned workforce
  - Changing workforce roles and responsibilities must be timed and coordinated with other programmatic element rollouts

Case Study – Changing Responsibilities for an ISSO

- Challenge
  - Information System Security Officers (ISSO) are expected to have a very broad-base of knowledge in both technology and business
  - Skillsets and LOE required for comprehensive system analysis beyond available resources
- Solution
  - Allow ISSOs to focus on what they do best – managing the business impacts and coordinating the needs of the System Owner
  - Supplement ISSO role with Security Engineer to rapidly solve security problems
- Benefits
  - Reduction in POAM Management LOE by 75%

Case Study – Learning How to Dynamically Manage IT Security Risk

- Challenge
  - Authorizing Officials (AO) and System Owners (SO) were not familiar with the dynamic, risk-based management approach created by the CM deployment model
- Solution
  - Specialized training for AOs, focusing on how to leverage the new Risk Management model for IT Security
- Benefits
  - Cost-informed management of IT security risks
  - Correlation and comparison of technology risks with financial, schedule and other organizational risk categories

Lessons Learned through our CM Program Deployment

Understanding the IT Security workforce, and working with its members to deploy a Continuous Monitoring program, are essential elements to a successful project.

- Capitalize on existing skillsets of the workforce, and focus training on the gaps created by change
- Deploy capabilities over time; spread out program elements so that supporting staff and stakeholders become comfortable with their new roles
- Train, train and retrain! Continued delivery of the new content over a period of time helps the message sink in

United States Census Bureau