Deloitte.

Operationalizing Continuous Monitoring

Almaz Tekle
Christian Neeley

November 2, 2011

Introduction

Challenges and Considerations

Discussion

- Monitoring What Matters
- Tailoring a Transition Plan
- Workforce Alignment
- Continuous Assessment & Vulnerability Data Management

Questions

From Compliance to Risk Based Monitoring

Check-the-box approach driven by compliance requirements	→	*Risk based* approach driven by mission strategic goals and priorities
Cyclical annual or 3-year C&A assessment, focused on *a point-in-time* security	→	*Continuous monitoring* of key security controls associated with identified risks
Tests all controls – focused on assessment of every security control (coverage)	→	*Prioritized testing of controls* – focused on assessment of essential security controls (effectiveness)
Siloed – C&A process lives in a rigid framework with little interaction with other organizational processes and operations	→	*Integrated* – provides opportunities for reuse, cost reduction, and a culture of security awareness

Challenges in moving to CM

- Organizations are faced with maintaining ongoing C&A while standing up a new CM Process with limited funds
- Transformation must leverage useful processes and artifacts of traditional C&A as well as other functions such as IT operations
- Need to determine what of the old C&A stays as-is, what goes away, what gets updated, and what new functions get added

Challenges in moving to CM

Am I focused in addressing the critical risks?

Do I have buy-in from stakeholders?

What controls do I assess and how often?

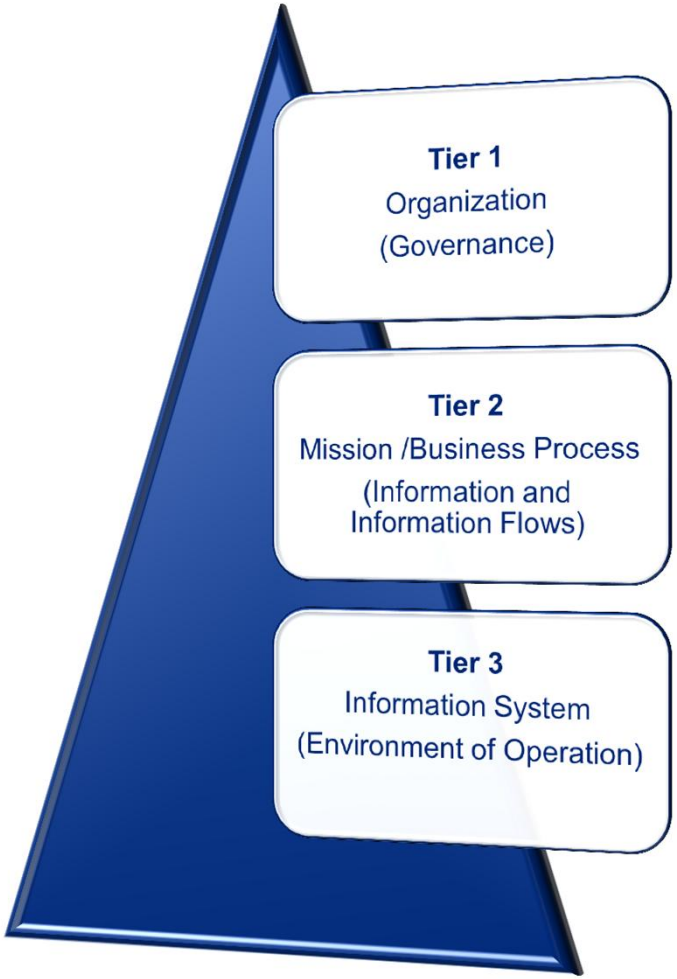
What tools must I purchase?

Is this plan right for *my* agency?

Am I putting my resources in the right place?

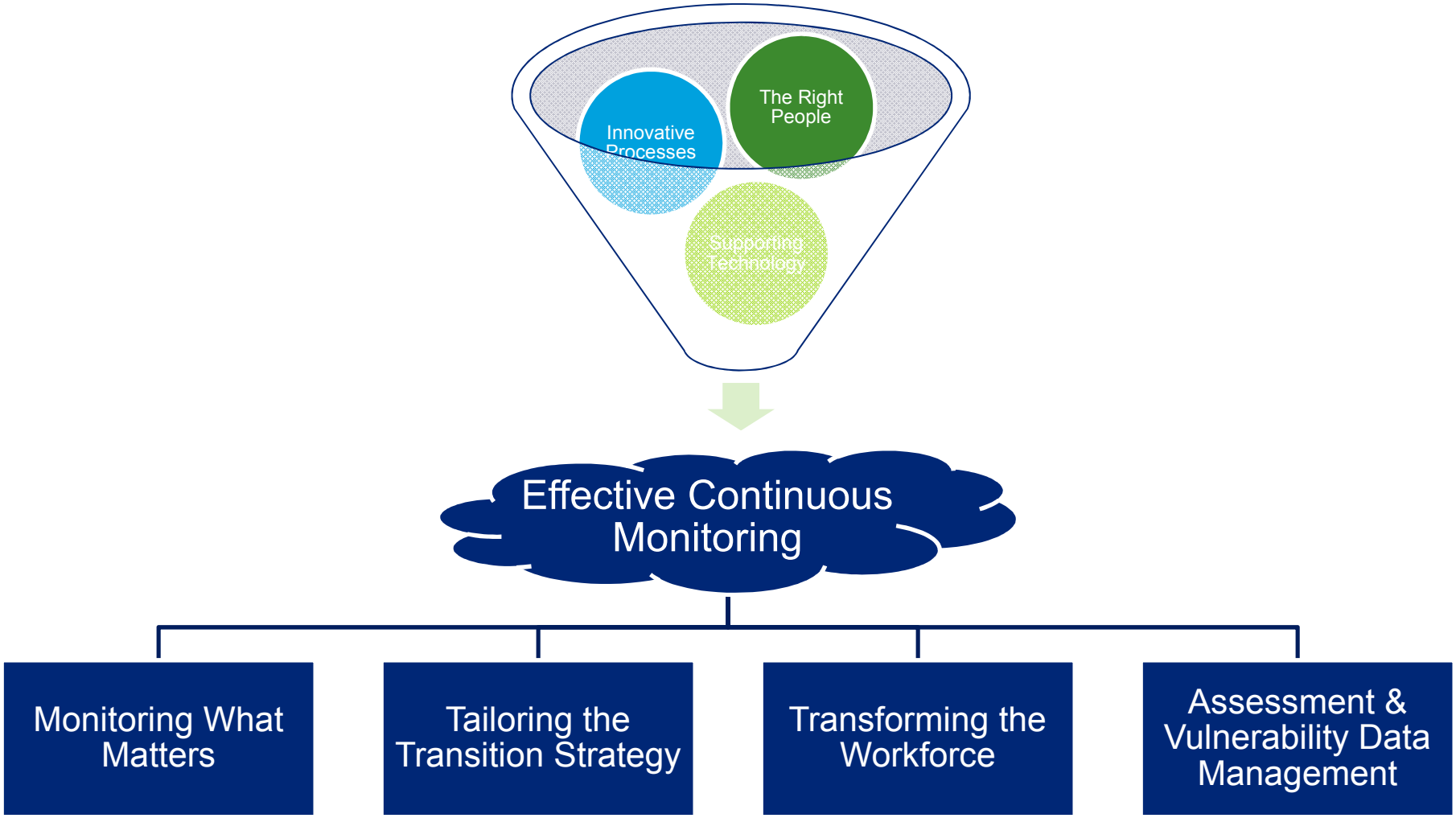
Is my workforce prepared for CM?

Considerations for CM Deployment



1. Develop a strong Transition Plan
2. Establish Governance in support of the process
3. Manage the change within the transformation
4. Confirm the Agency Baseline and Configuration Standards
5. Monitor controls based on business and technology Risk
6. Align the workforce to support system security functions
7. Learn from other businesses and agencies actions
8. Establish an automation infrastructure for assessments
9. Integrate Security into Architecture and the SDLC

The Challenges Posed by Continuous Monitoring Deployment



Challenge #1 – What do I Monitor and How Often?

Prioritizing security control monitoring and allocating resources to your high risk assets is essential.

1) Every agency is unique. Your important and high value assets are likely not the same as your neighbor's
   - Choose a risk framework that allows unique agency characteristics drive the CM approach that you take
   - Never forget the mission – your business should remain front-and-center in the risk equation
2) Leverage the achievements of other industries in modeling and targeting various risk scenarios
   - Organizations in finance, energy, and international relations have developed risk models that can be easily adapted for CM
   - Let the good work of those who came before us support and inform your risk determination framework

Challenge #1 – What do I Monitor and How Often?

What's my potential for ROI?

- ✓ Targeting risky assets allows for maximization of efficiency for every security dollar expended
  - Case Study – Continuous Monitoring assessment frequency analysis
    - Assessment frequency can be based on system use, mission, and technology factors
    - Justifies system-specific continuous monitoring plans that can better align overall agency expenditure of effort

Challenge #2 – Tailoring to a Transition Plan

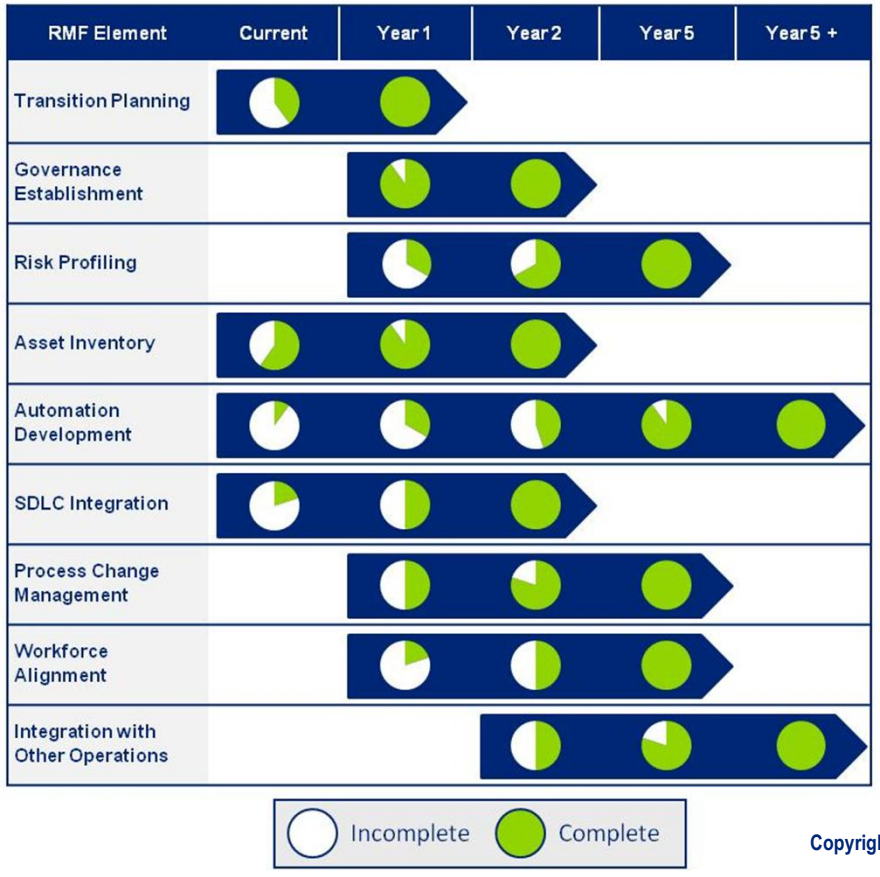
Demonstrating continued compliance with current federal regulations is essential to bring credibility to a new CM process:

1) Start from a position of strength
2) Engage key stakeholders
3) Identify early adopters / potential pilot programs
4) Pick a pilot with the highest potential for success

Challenge #2 – How do I Get From C&A to CM?

What's my potential for ROI?

- ✓ Understanding your existing organization and repurposing capabilities reduces costs and time-to-deploy for CM programs
  - Case Study – Transition Planning Analysis



Challenge #3 – Is My Workforce Ready for the Change?

For a successful CM rollout, prepare your workforce for CM by managing their expectations and supporting their development needs

1) Understand the scope and capabilities of your IT workforce
   - Find out who is really available to support the CM processes. Employees outside of the security organization are often overlooked yet valuable resources
   - Understand the technology, policy, planning, engineering, etc. requirements of your CM program and analyze and understand the strengths and weaknesses of your human capital in supporting the program
2) Tailor processes and program outputs to capitalize on staff strengths
   - Develop a cross functional and unified view of constituent components of CM. Consider moving responsibilities across functional lines in order to realize process efficiency
   - Set your workforce up for success. Assign staff members goals and responsibilities that they are prepared to meet and exceed.

Challenge #3 – Is My Workforce Ready for the Change?

What's my potential for ROI?

- ✓ Appropriate assignment of roles can drive double-digit decreases in vulnerability mitigation LOE
  - Case Study – ISSO issue remediation analysis
    - Sample agency stands to realize 75% reduction in cost for issue remediation

Challenge #4 – What Do I Do With All of this Data?

Vulnerability and configuration data add up quickly. Regularly making use of that information is foundational to CM

1) CAESARS has set the stage for configuration data collection and management – USE IT
   - Idealistic notions of all-in-one assessment tools fail to capitalize on technology investments already supported by the agency
2) Cyberscope reporting is mandatory, but don't just throw the data over the fence
   - Basic risk information is inherent to configuration data, but the real benefit comes from correlating that data across disparate processes and systems
   - SEIM-based triggers and structured analysis of bulk configuration data can help you cut through the noise to find the melody

Challenge #4 – What Do I Do With All of this Data?

What's my potential for ROI?

- ✓ Aggregating and correlating existing data sources can rapidly increase compliance management and vulnerability identification and issue reporting
  - Case Study – Simplified reporting and data reuse
    - Sample agency capitalized on existing operations toolsets, saving a $1.5M investment in new compliance management tools

What to Expect – And Watch Out For

Demonstrating continued compliance with current federal regulations is essential to bring credibility to a new CM process:

1) Reporting capabilities become immediately critical to both representing system risk during the transition and allowing for continuous system authorization
   - Establish core metrics and reporting capabilities to begin flowing risk information to Authorizing Officials on regular cycles
2) Core C&A documentation (as existed previously) still has a purpose
   - CM can be a powerful tool to understand and manage an agency's risk posture; however, we're still bound by some basic rules of compliance that influence our actions
3) Cost control in the CM world will make or break your program. Make sure you can justify where you spend your dollars

This presentation contains general information only and Deloitte is not, by means of this presentation, rendering accounting, business, financial, investment, legal, tax, or other professional advice or services. This presentation is not a substitute for such professional advice or services, nor should it be used as a basis for any decision or action that may affect your business. Before making any decision or taking any action that may affect your business, you should consult a qualified professional advisor.

Deloitte, its affiliates and related entities shall not be responsible for any loss sustained by any person who relies on this presentation.

As used in this document, “Deloitte” means Deloitte & Touche LLP, a subsidiary of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries. Certain services may not be available to attest clients under the rules and regulations of public accounting.

Contact Us

Almaz Tekle
Principal
Deloitte & Touche LLP
+1 301.502.8839
atekle@deloitte.com

Christian Neeley
Senior Manager
Deloitte & Touche LLP
+1 703.967.7791
cneeley@deloitte.com