Homeland Security

Continuous Diagnostics and Mitigation
Webinar Series

CDM Roles and Responsibilities

A CDM Learning Community Event

February 11, 2016

Welcome

Quick Notes

- Due to technical restrictions, we are unable to open the phone line, thus the audio is in listen only mode
- Use the chat box to send comments, questions – we want to hear from you!
- Headphones are recommended to resolve audio issues

Introduction of Facilitators

- Ms. Susan Hansche
  - Training Manager, DHS Federal Network Resilience
  - Over 25 years of experience in the training field
  - Past 17 years focus on building information system security training programs
  - Author of “The Official (ISC)2 Guide to the CISSP Exam”
  - Author of “The Official (ISC)2 Guide to the ISSEP CBK”
  - 2011 FISSEA “Educator of the Year Award”

- Mr. Jim Wiggins
  - Cybersecurity Trainer and Information Security Practitioner
  - 18 years of experience in IT
  - 14 years of experience in IT security
  - Contractor supporting the Federal Network Resilience division at DHS
  - 2010 FISSEA “Educator of the Year Award”

Introduction

- Overview of CDM Program Concepts
- CDM Roles and Responsibilities Guide Overview
- Mapping CDM Roles to RMF Tiers
  - Tier 1 – Organization
  - Tier 2 – Mission/Business Process
  - Tier 3 – Information Systems
- Summary
- Questions and Answers

Webinar Rhythm

Extending the Dialogue

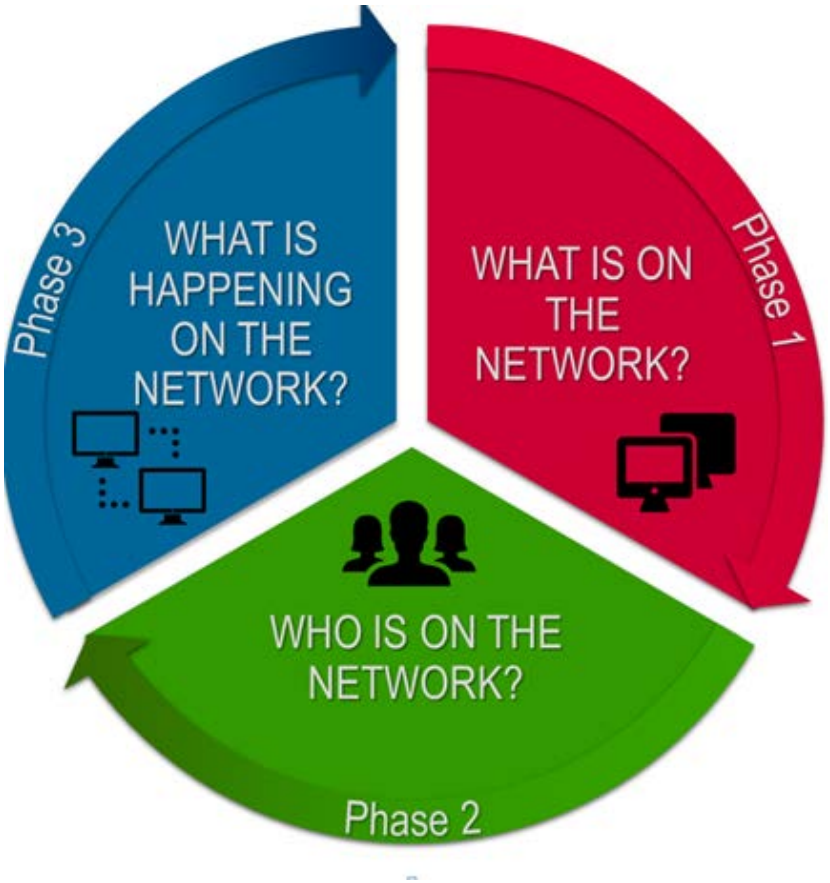
- Polling questions related to your operational environment
- Use chat feature to add comments
- Use chat feature to ask questions
- Use chat feature to share your best practices

Basic Overview of the CDM Program

What is the CDM Program?

- Establish consistent, government-wide set of information security continuous monitoring tools to help protect .gov networks.
- Leverage the buying power of government organizations to achieve savings for cybersecurity tools and services.
- Provide dashboards to improve situational awareness, enhance agencies' ability to identify, and respond to risk of emerging cyber threats on the agency and government-wide level.
- Supports risk-based decision making for resource allocation.

Basic Overview of the CDM Program



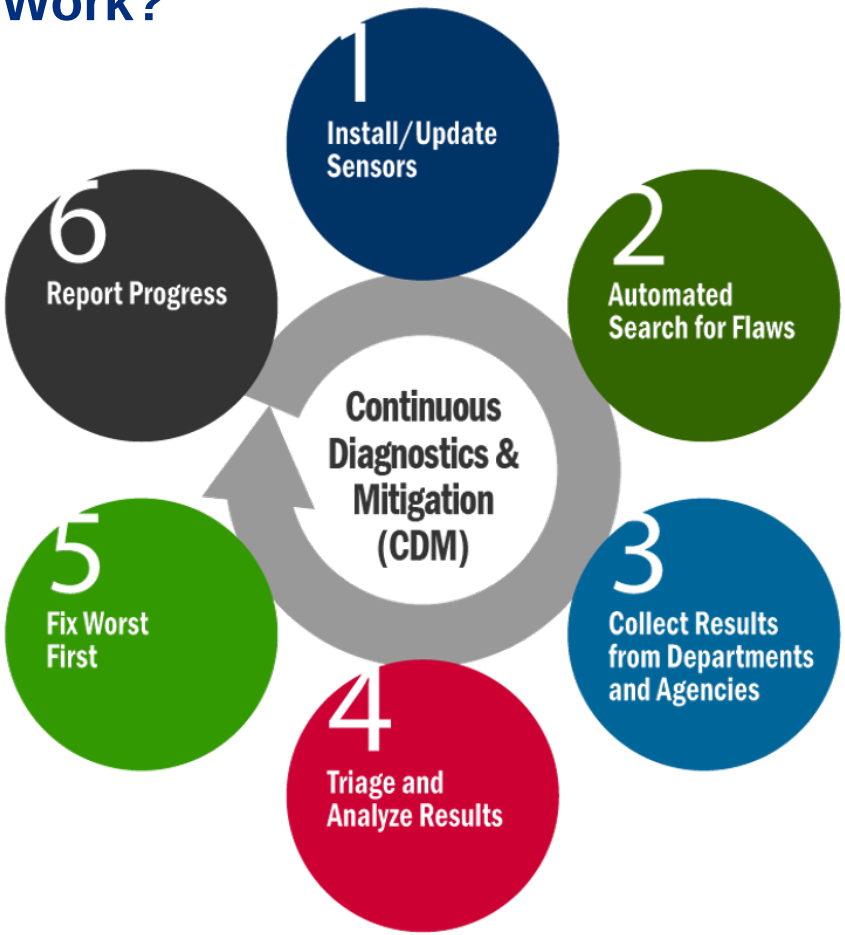
What is on the Network?

Who is on the Network?

What is Happening on the Network?

Basic Overview of the CDM Program

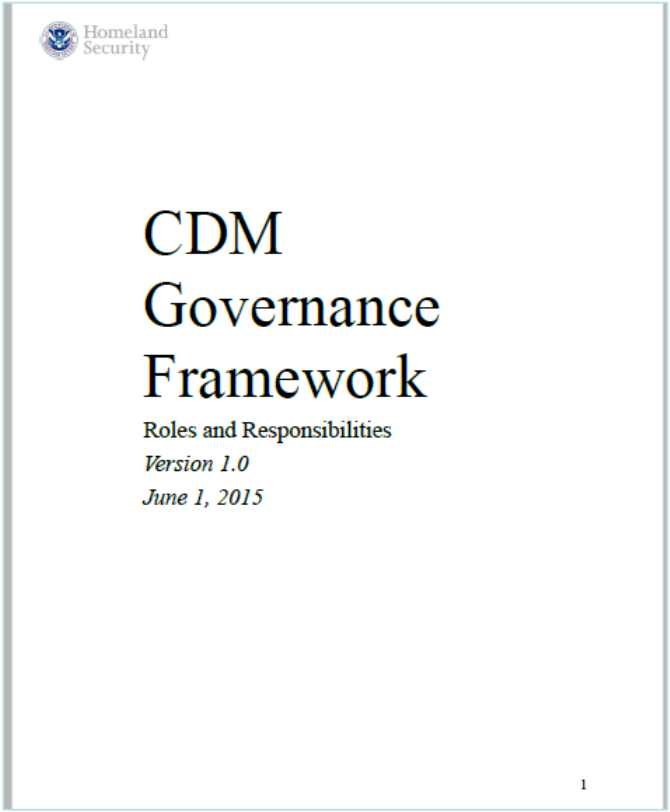
How does it Work?



CDM Roles and Responsibilities (R&R) Guide Overview

Purpose

- Guidance on how CDM Program impacts decision making
- Guidance on R&R of stakeholders for successful deployment, operation, and maintenance of CDM program into existing processes and procedures
- Does not mandate R&R requirements within a D/A


Homeland Security

CDM Governance Framework

Roles and Responsibilities

Version 1.0

June 1, 2015

1

Key Elements

A successful CDM Program relies on:

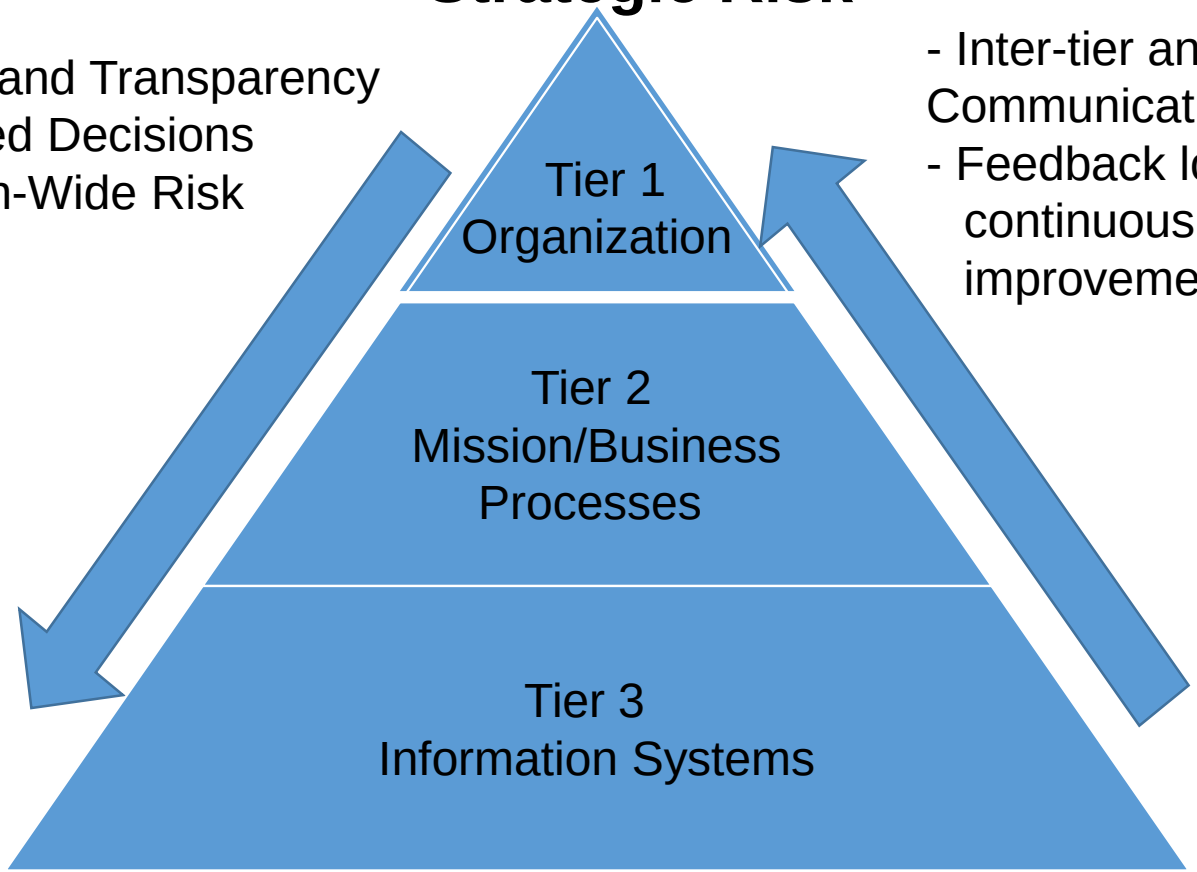
- Communications – a foundational enabler of successful security management
- Training – to ensure a common understanding of CDM concepts and principles
- Workforce - linked to training, the workforce must shift focus from paper-based compliance to risk-based diagnostics and mitigation

Mapping CDM Roles to RMF Tiers

NIST SP 800-37 Multi-Tiered Risk Management Framework

Strategic Risk

- Traceability and Transparency of Risk-Based Decisions
- Organization-Wide Risk Awareness



- Inter-tier and Intra-tier Communications
- Feedback loop for continuous improvement

Tactical Risk

Tier 1 – Organization Governance

NIST 800-37 Tier 1 Scope

- **Comprehensive governance structure and organization-wide risk management strategy:**
- (i) the techniques and methodologies the organization plans to employ to assess information system-related security risks and other types of risk of concern to the organization;
- (ii) the methods and procedures the organization plans to use to evaluate the significance of the risks identified during the risk assessment;
- (iii) the types and extent of risk mitigation measures the organization plans to
- employ to address identified risks;
- (iv) the level of risk the organization plans to accept (i.e., risk tolerance);
- (v) how the organization plans to monitor risk on an ongoing basis given the inevitable changes to organizational information systems and their environments of operation;
- (vi) the degree and type of oversight the organization plans to use to ensure that the risk management strategy is being effectively carried out.

Tier 1 – Organization Governance

- **NIST 800-37 Tier 1**
- **Focus is "Strategic risk"**
- **Comprehensive governance structure and organization-wide risk management strategy**

CDM Roles and Responsibilities

"Without clearly defined authority, decisions may not be made in a timely and attributable manner.."

Without documented decision-making processes, the validity of specific decisions will be inherently uncertain or undefined..

Without accountability, decisions will lack transparency and will constrain effective program management and performance measurement."

– DHS CDM R&R Guide

Tier 1 – Organization Governance

Specific Roles and Responsibilities

"The risk management strategy is propagated to organizational officials and contractors with programmatic, planning, developmental, acquisition, operational, and oversight responsibilities"

Authorizing Official

Chief Information Officer

Risk Executive Function

<u>CDM connection:</u>
The DHS CDM R&R Guide recommends that Tier 1 should establish the continuous monitoring strategy and how the strategy will fit into the organization's existing information security structure.

Tier 2 – Mission/Business Process

NIST 800-37 Tier 2 Scope

Comprehensive Mission/Business Structure Strategy:

i. Define the mission/business processes needed to support the missions and business functions of organizations

ii. Prioritize the mission/business processes with respect to the strategic goals and objectives of the organization

iii. Define the types of information needed to successfully execute the mission/business processes, the criticality/sensitivity of information, and the internal and external information flows of organizations

iv. Incorporate information security requirements into the mission/business processes

v. Establish an enterprise architecture with embedded information security architecture that promotes cost-effective and efficient information technology solutions consistent with strategic goals and objectives of the organization and measures of performance.

Tier 2 – Mission/Business Process

Risk-Aware Mission/Business Processes

Types of Threat Sources and Events	Potential Adverse Impacts on the Organization	Realistic Resilience Expectations

Enterprise Architecture

Provide Clarity and Understanding of IT Infrastructure	Standardizes, Consolidates, and Optimizes IT Assets	Segmentation, Redundancy, and Elimination of Single Point of Failure

Information Security Architecture

Information System Resilience and Architecting the Security Capabilities	Incorporates Security Requirements from legislation, directives, policies, etc.	Provides a Roadmap from Strategic Goals to Information Security Solutions

Tier 2 – Mission/Business Process

CDM R&R Guide

Chief Information Security Officer (CISO)
Senior Information Security Officer (SISO)
Information System Security Officer
Common Control Provider
Control Assessor/Auditor
RMF Program Manager
ISCM and CDM Managers
Local Scoring and Metrics Group

<u>CDM connection:</u>
The DHS CDM R&R Guide recommends that Tier 2 should establish the continuous monitoring implementation processes and coordinate reporting structures to ensure decision makers have visibility into the risks, thus making better risk management decisions.

Tier 3 – Information Systems

NIST Tier 3 Scope:

Comprehensive Information Systems Strategy:

i. Categorizing organizational information systems

ii. Allocating security controls to organizational information systems and environments in which those systems operate consistent with the organization's established enterprise architecture and embedded information security architecture

iii. Managing the selection, implementation, assessment, authorization, and ongoing monitoring of allocated security controls as part of a disciplined and structured system development life cycle process implemented across the organization

Tier 3 – Information Systems

Initiation

- Information System Requirements
- Functional Requirements
- Security Functionality

Development/Acquisition

- Supply Chain Risk
- Environmental Risk

Implementation

- Effectiveness of Security Capabilities prior operations
- Actual/Desired State Comparison prior operations

Operations/Maintenance

- Monitoring Security Capabilities
- Defect Mitigation

Disposal

- Removal of Unauthorized Assets
- Risk Assessment

Tier 3 – Information Systems

CDM Roles and Responsibilities

Information System Owner (ISO)
Information Owner/Steward
Information System Security Officer
System Administrators
Mitigators
Organizational Help Desk

<u>CDM connection:</u>
The DHS CDM R&R Guide recommends that Tier 3 should use the data from the dashboard to assess risk on an ongoing basis; respond to defect check data, and, if appropriate, mitigate the risk.

Recap

The effective execution of the CDM Program requires collaboration across multiple activities and among numerous stakeholders. At a high level, the DHS CDM Program consists of three inter-dependent activity sets:

- Acquisition: acquiring CDM sensors, services, and dashboards
- Implementation: deployment of CDM sensors, services, and dashboards
- Operations: operation of the sensors as well as management of the CDM dashboard to identify, prioritize, and inform mitigation of and oversight of systemic cybersecurity risks

Recap

Each of these activities encompass specific program management requirements.

In order to achieve successful CDM management, planning, implementation, and maintenance, organizations must function together across all tiers.

The R&R guide provides initial guidelines to facilitate CDM deployment – it will be revised as the program develops.

Must be tailored to meet the requirements of your organization.

Comments on the R&R guide can be sent to the CDM Learning Program office at cdm.fnr@dhs.gov

Additional Resources

GSA Site

- http://www.gsa.gov/cdm

CDM Learning Program Site

- http://www.us-cert.gov/cdm

Additional Upcoming Activities

- February 18th CDM Learning Community Event - CDM and the RMF: Making it Work

CDM PMO Program Managers

No discussion or questions regarding CDM acquisition or procurement activities– this is strictly a CDM learning community activity. For agency-specific queries, contact:

Group A – DHS

- Betsy Proch (betsy.proch@hq.dhs.gov)

Group B – DOE, DOI, DOT, USDA, VA, OPM

- Derrick Williams (derrick.Williams@hq.dhs.gov)

Group C – DOC, DOJ, DOL, State, USAID

- Paul Loeffler (paul.loeffler@hq.dhs.gov)

Group D – GSA, HHS, NASA, SSA, Treasury, USPS

- Odell Blocker (odell.blocker@hq.dhs.gov)

Group E – Educ, EPA, HUD, NRC, NSF, SBA

- Matt Hartman (matthew.Hartman@hq.dhs.gov)

Group F – Non-Chief Financial Officer (CFO) Act Agencies

- Geri Clawson (geraldine.clawson@hq.dhs.gov)

Unsure?

- CDM.FNR@hq.dhs.gov

Contact Information

THANK YOU FOR ATTENDING OUR FEBRUARY WEBINAR.

Contact:
cdm.fnr@hq.dhs.gov