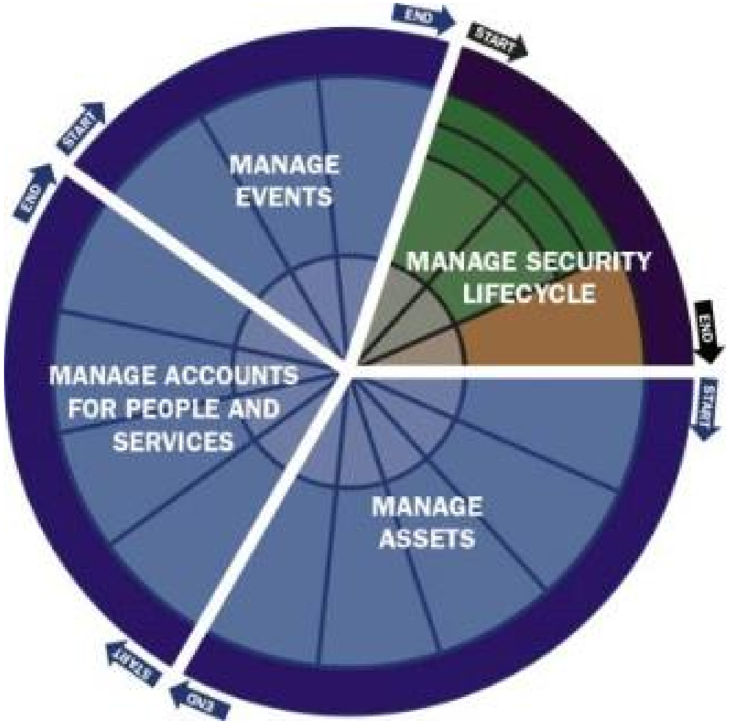
Homeland Security

# Continuous Diagnostics and Mitigation

## Update, Interagency Communications, and Agency Involvement


END
START
START
END
MANAGE EVENTS
MANAGE SECURITY LIFECYCLE
END
START
MANAGE ACCOUNTS FOR PEOPLE AND SERVICES
MANAGE ASSETS
START
END

August 17, 2016

# Introduction

Ms. Susan Hansche

- Training Manager, DHS Federal Network Resilience
- Over 25 years of experience in the training field
- Past 18 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”

# CDM PMO Program Managers

## 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**

- Derek Adams **(derek.adams@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

# Overview of the CDM Program

CDM is one method to achieve the goal of information security continuous monitoring.

CDM provides enabling tools.

CDM provides visibility into the state of the network assets.

Who are they enabling? And, to do what?

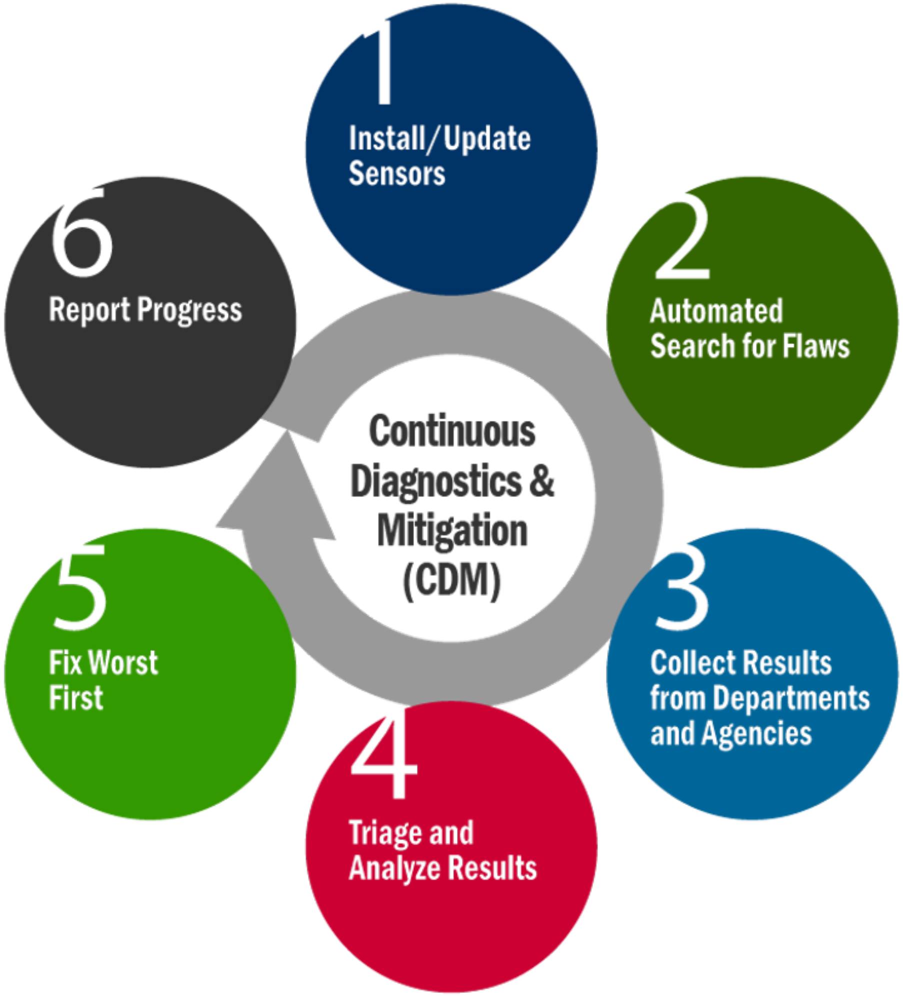
# Overview of the CDM Program

What is the CDM Program?

- Establish consistent, government-wide set of continuous monitoring tools to help protect .gov networks.
- Provide dashboards that:
  - provide visibility into the “state” of the network assets
  - improve situational awareness
  - enhance agencies’ ability to identify, and respond to risk of emerging cyber threats
  - support decision-making related to risk management, compliance and performance, and security functions.

# Basic Overview of the CDM Program

## How does it work?



Continuous Diagnostics & Mitigation (CDM)

1 Install/Update Sensors

2 Automated Search for Flaws

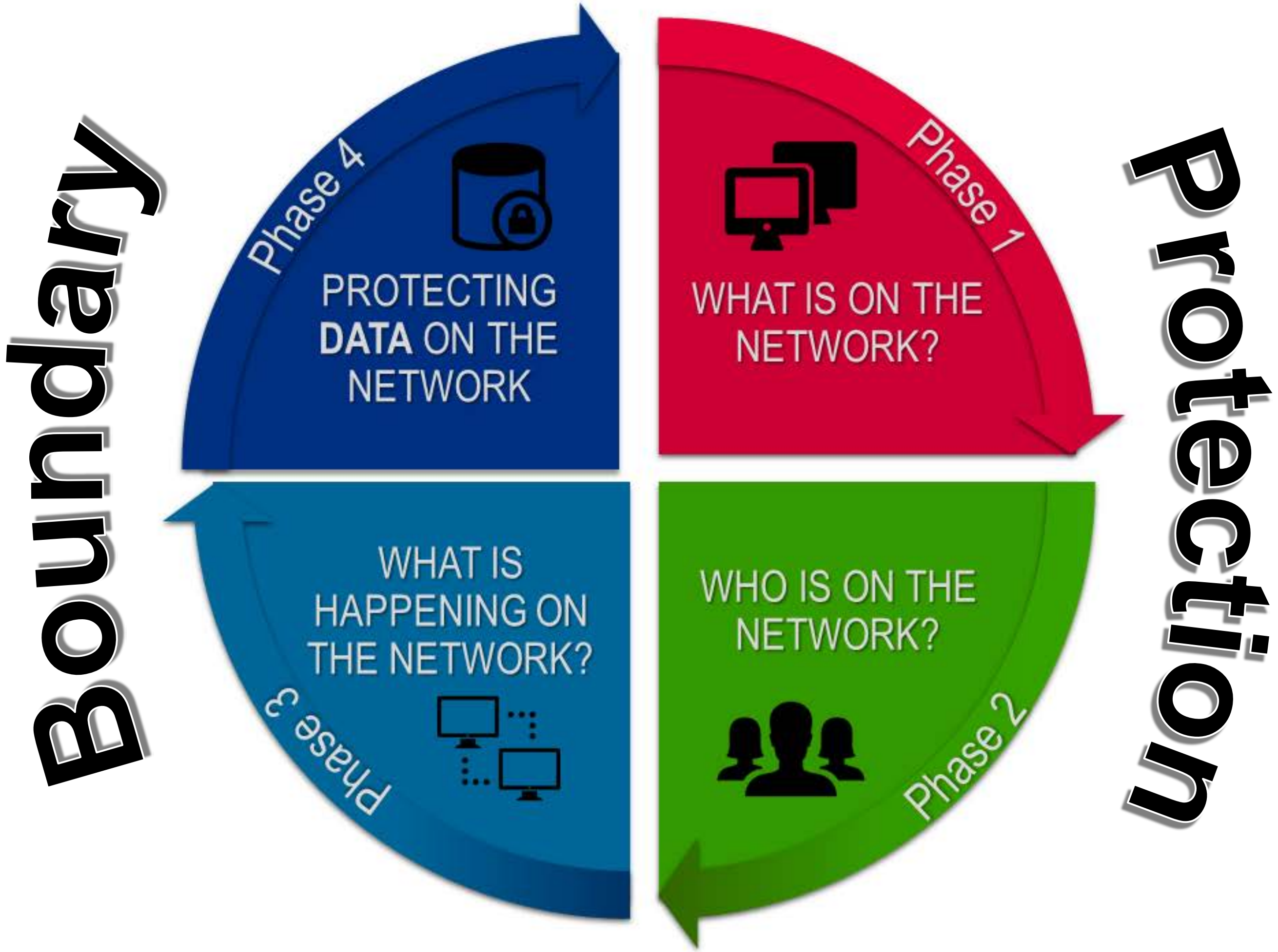
3 Collect Results from Departments and Agencies

4 Triage and Analyze Results

5 Fix Worst First

6 Report Progress

# Basic Overview of the CDM Program



# Your Role

## 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

# Your Role in Continuous Monitoring

How well do you understand your role in the CDM program management, planning, and implementation?

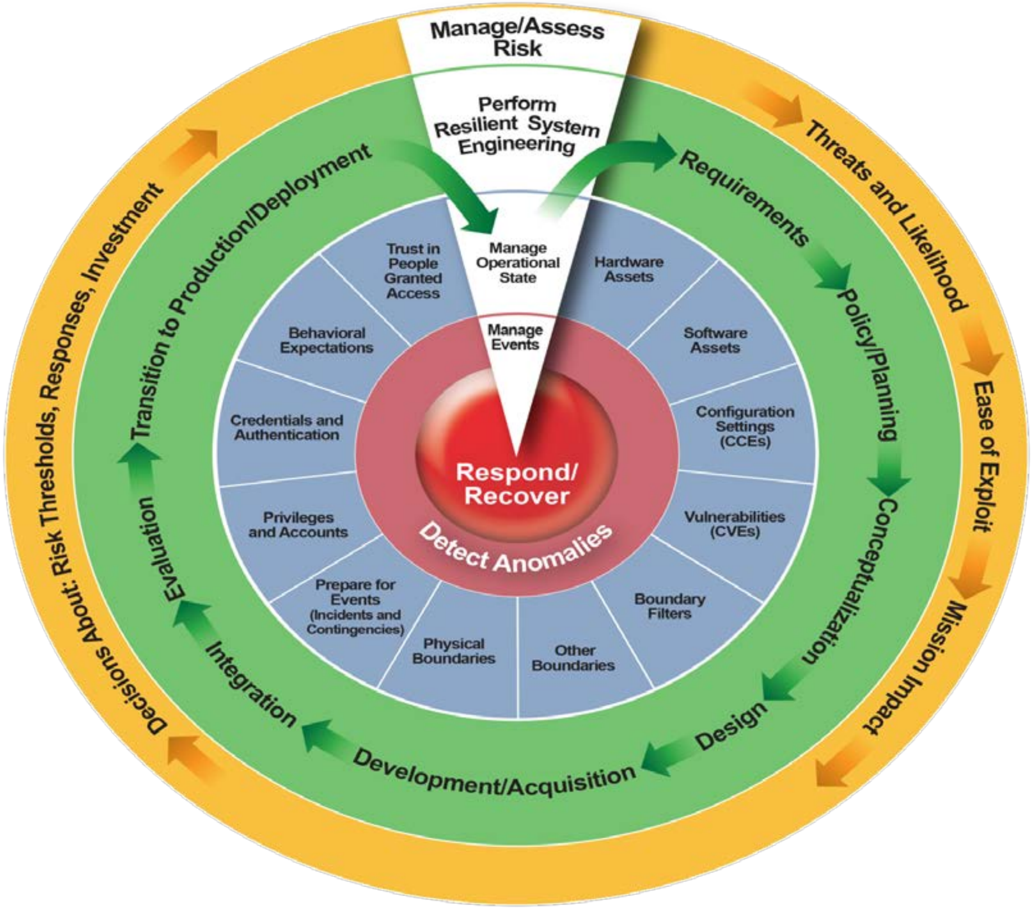
a. Very well
b. Well
c. Not so well
d. Not at all
e. I’m still trying to understand CDM
f. Other …

# Your Role in Continuous Monitoring

How well do you understand the role of other personnel or groups within your organization with regards to CDM program management, planning, and implementation?

a. Very well
b. Well
c. Not so well
d. Not at all
e. I’m the only who is doing this
f. Other …

# Your Role in Continuous Monitoring



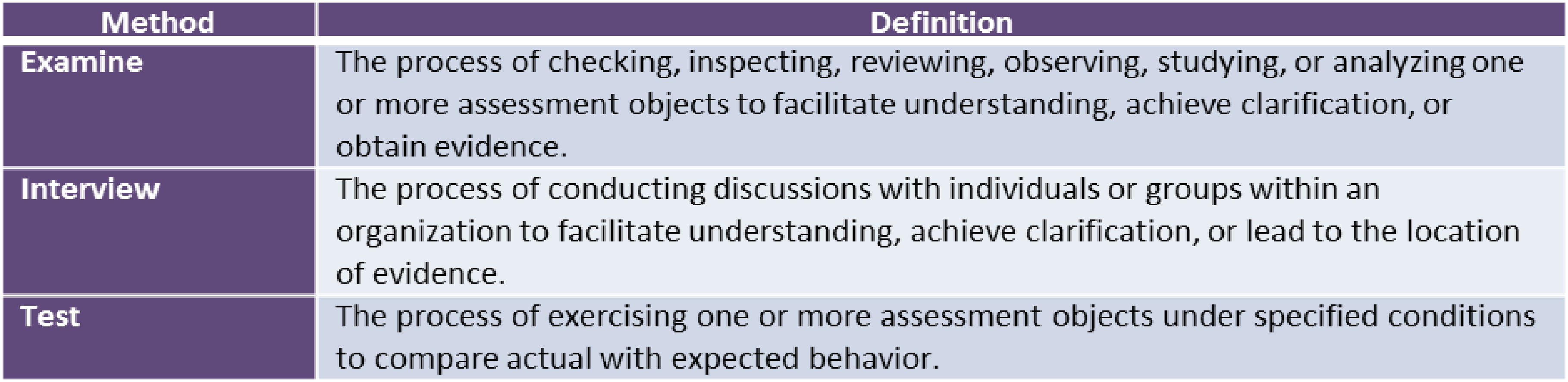
PREPARATION BEGINS WITH UNDERSTANDING YOUR EXISTING NIST SP 800-53 CONTROLS

As suggested by SP 800-53A Rev 4, security *capabilities* are groups of security controls working together to support a particular *purpose*.

# Your Role in Continuous Monitoring

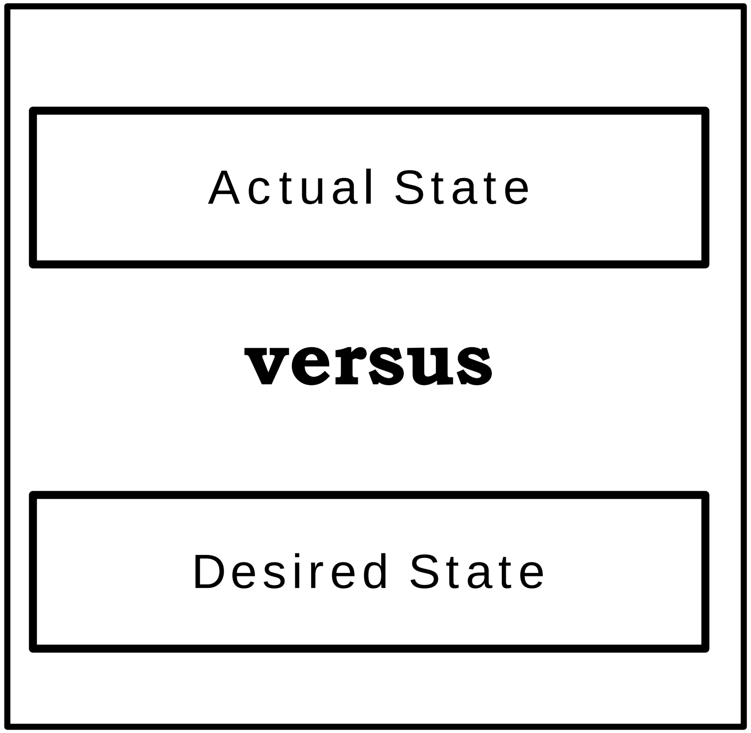
- Think about how automation will impact the “Testing” of security control implementation (not examine or interview)

PREPARATION BEGINS WITH UNDERSTANDING YOUR ASSESSMENT METHODS



| Method | Definition |
|---|---|
| **Examine** | The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. |
| **Interview** | The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. |
| **Test** | The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. |

# Know Your Desired State



Actual State

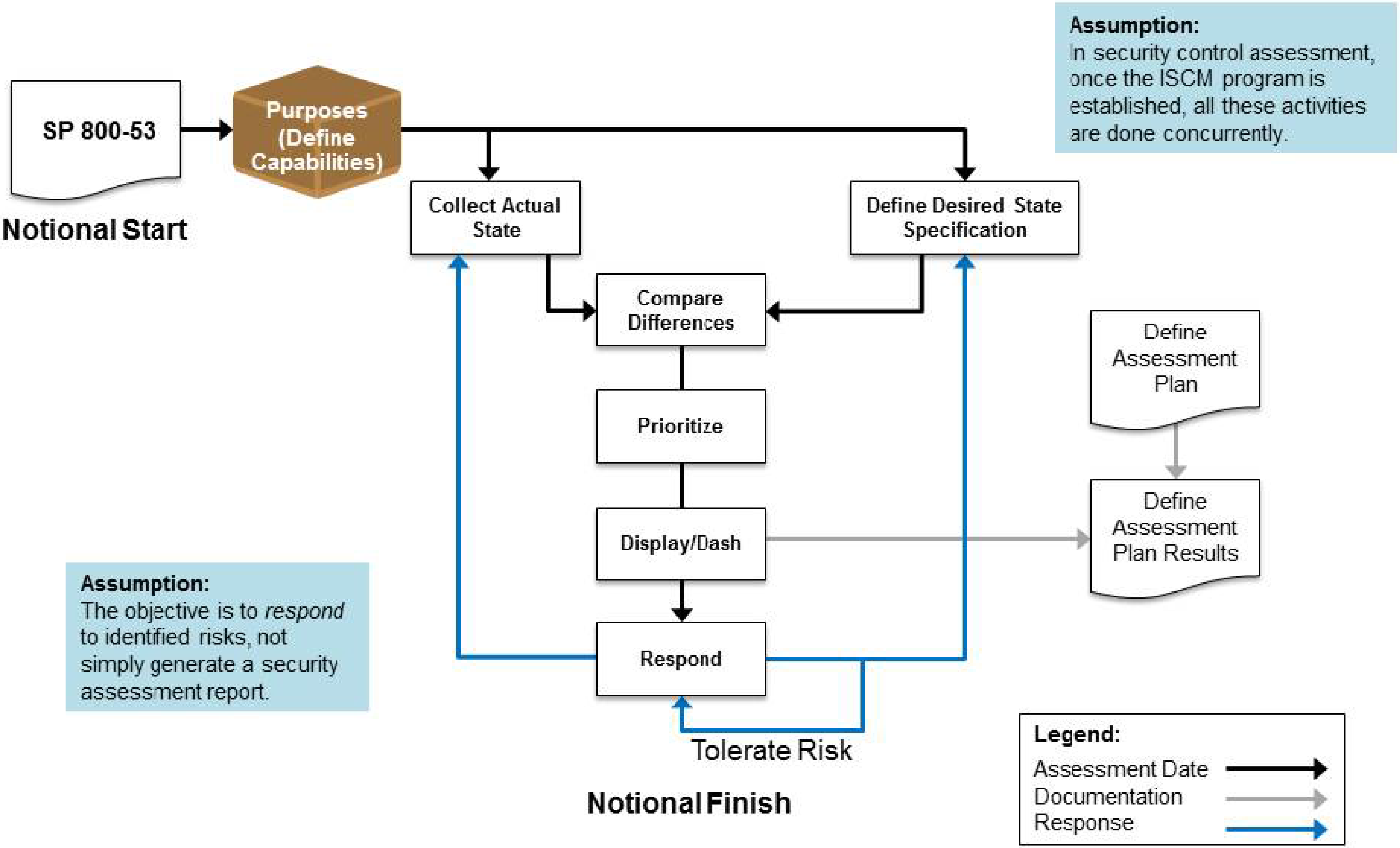
**versus**

Desired State

PREPARATION BEGINS WITH UNDERSTANDING YOUR DESIRED STATE

Automated assessments (in the form of defect checks) are performed, using the ***test assessment*** method defined in SP 800-53A, by comparing a desired and actual state (or behavior).

# Understand Existing Actual and Desired State

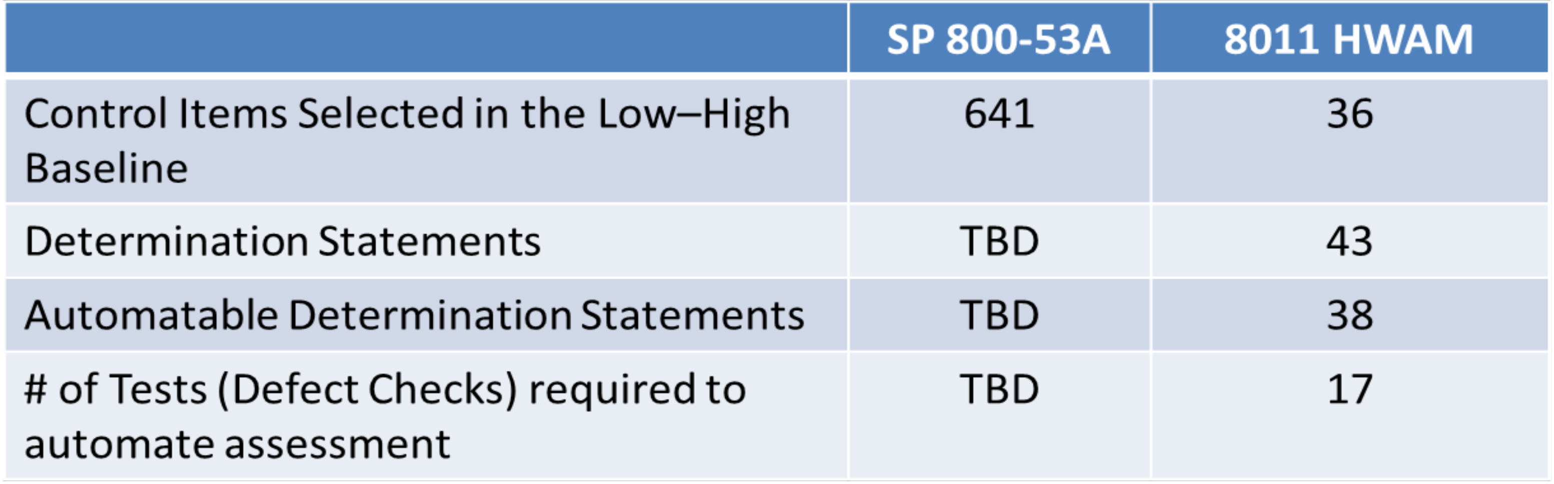


**Assumption:**
In security control assessment, once the ISCM program is established, all these activities are done concurrently.

**Assumption:**
The objective is to *respond* to identified risks, not simply generate a security assessment report.

# Understanding Automated Assessment

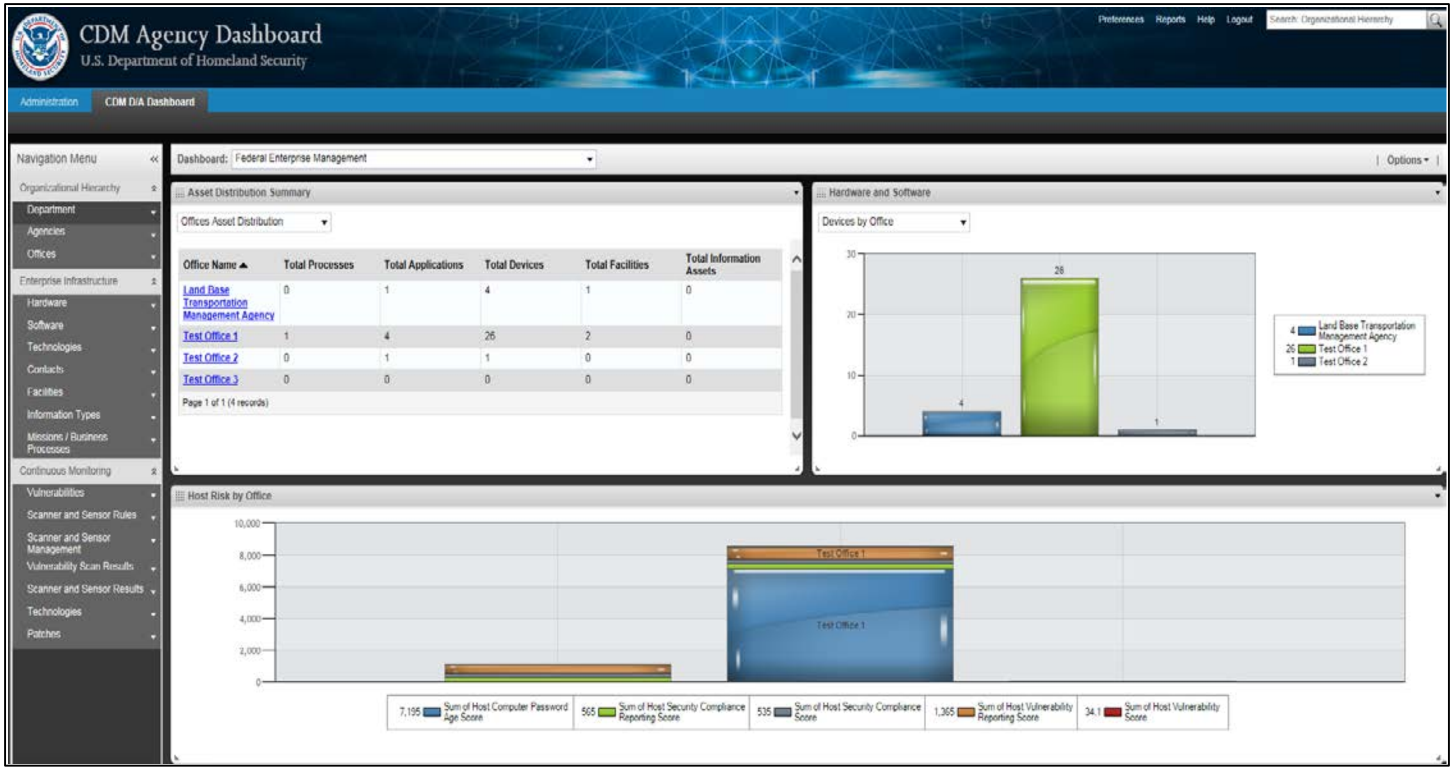
A key feature of the 8011 approach to automated assessment is that it makes it unnecessary to test determination statements for each control individually—if the defect check for the sub-capability passes, then it is concluded that the controls supporting it are also effective.



| | SP 800-53A | 8011 HWAM |
|---|---|---|
| Control Items Selected in the Low–High Baseline | 641 | 36 |
| Determination Statements | TBD | 43 |
| Automatable Determination Statements | TBD | 38 |
| # of Tests (Defect Checks) required to automate assessment | TBD | 17 |

For HWAM, then, 38 of 43 determination statements (88%) can be automated, and only 17 defect checks are required to see if the purposes of the HWAM capability are being met—a sizable reduction in required testing.

# The Dashboard – The Visibility Portal



Dashboard: Federal Enterprise Management

Offices Asset Distribution

| Office Name ▲ | Total Processes | Total Applications | Total Devices | Total Facilities | Total Information Assets |
|---|---|---|---|---|---|
| Land Base Transportation Management Agency | 0 | 1 | 4 | 1 | 0 |
| Test Office 1 | 1 | 4 | 26 | 2 | 0 |
| Test Office 2 | 0 | 1 | 1 | 0 | 0 |
| Test Office 3 | 0 | 0 | 0 | 0 | 0 |

Page 1 of 1 (4 records)

| | | |
|---|---|---|
| 4 | 🟦 | Land Base Transportation Management Agency |
| 26 | 🟩 | Test Office 1 |
| 1 | ⬛ | Test Office 2 |

| | | |
|---|---|---|
| 7,195 | 🟦 | Sum of Host Computer Password Age Score |
| 565 | 🟩 | Sum of Host Security Compliance Reporting Score |
| 535 | ⬛ | Sum of Host Security Compliance Score |
| 1,365 | 🟧 | Sum of Host Vulnerability Reporting Score |
| 34.1 | 🟥 | Sum of Host Vulnerability Score |

## RSA Archer eGRC

- Federal Enterprise Management Module
- Continuous Monitoring Module
- On-Demand Applications

# Some thoughts on what to do

- Define your desired state
- Begin planning “container” structures for FISMA systems
- Determine agency requirement for CDM Dashboard hierarchy
- Review policy and process impacts
- Understand the roles and responsibilities
- Develop a communications plan – who needs to know what and when
- Incorporate CDM into ISMC strategy

# Some thoughts on what to do

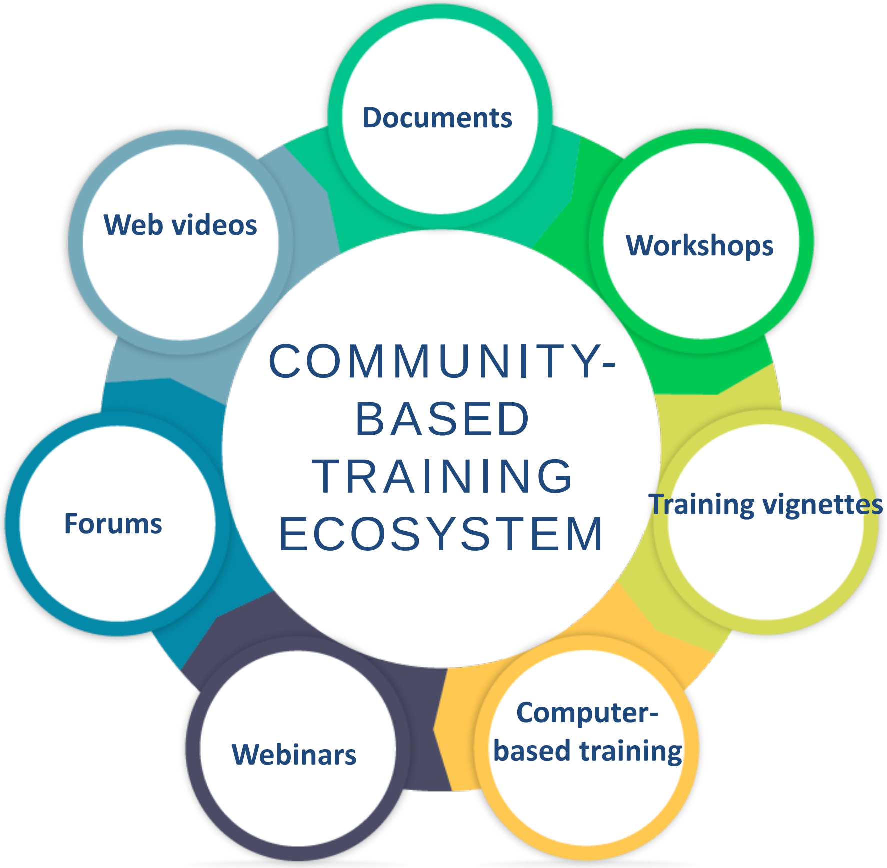
- A Technical Lead to facilitate PRIVMGMT discovery and implementation activities after the solution Design Review (SDR) in September.
- Your agency readiness and scheduling constraints in regards to PRIVMGMT.
- We recommend you consider establishing a PRIVMGMT Integrated Project Team (IPT) within your agency to facilitate Intra-agency communications.

*August 12 email from CDM.FNR*

# CDM Learning Program

Current Offerings

- Weekly Awareness Tip and Blog Posting
- Monthly Webinar Series
- Online vignettes
- Guides
- Online resources



# CDM Learning Program

## CDM Awareness Tips

## Bits and Bytes

**WHO:** Anyone and everyone

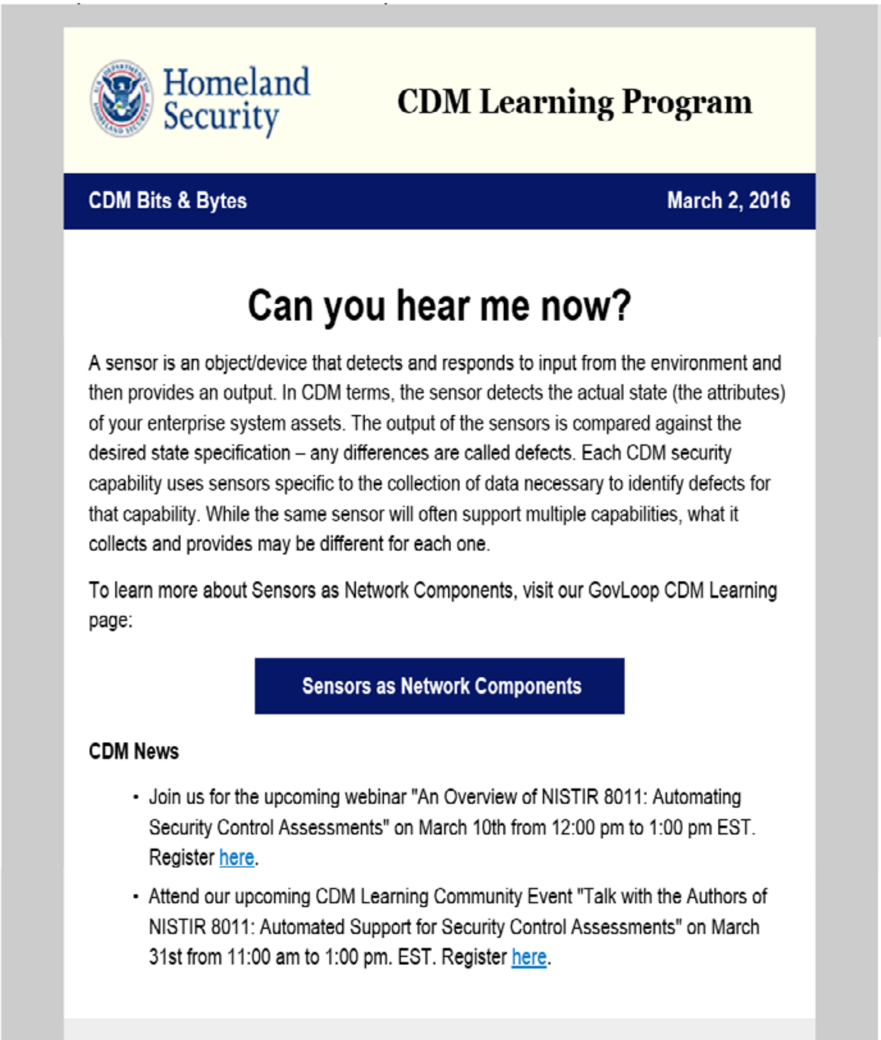
**WHAT:** Provide information on upcoming news, events, resources, and high level content

**WHERE**: Via email and blog

**WHEN:** Every Wednesday

**WHY:** To understand CDM principles to prepare for planning and implementation.

**HOW:** GovDelivery and GovLoop



Homeland Security

CDM Learning Program

CDM Bits & Bytes

March 2, 2016

### Can you hear me now?

A sensor is an object/device that detects and responds to input from the environment and then provides an output. In CDM terms, the sensor detects the actual state (the attributes) of your enterprise system assets. The output of the sensors is compared against the desired state specification – any differences are called defects. Each CDM security capability uses sensors specific to the collection of data necessary to identify defects for that capability. While the same sensor will often support multiple capabilities, what it collects and provides may be different for each one.

To learn more about Sensors as Network Components, visit our GovLoop CDM Learning page:

Sensors as Network Components

CDM News

- Join us for the upcoming webinar "An Overview of NISTIR 8011: Automating Security Control Assessments" on March 10th from 12:00 pm to 1:00 pm EST. Register here.
- Attend our upcoming CDM Learning Community Event "Talk with the Authors of NISTIR 8011: Automated Support for Security Control Assessments" on March 31st from 11:00 am to 1:00 pm. EST. Register here.

# CDM Learning Program

## Monthly Webinar Series

**WHO:** IT Operations and Mgmt, IT Security

**WHAT**: One-hour webinar to provide information on CDM topics and related concepts

**WHERE:** Online

**WHEN:** 2nd Thursday of each month, 12:00pm – 1:00pm

**WHY:** Be better prepared for CDM planning and implementation

**HOW:** HSIN Connect

**August 18**, 12:00-1:00pm
ISCM Foundations: Understanding CDM's CSM Security Capability

**September 15**, 12:00-1:00pm
ISCM Foundations: Understanding CDM's CSM Security Capability

# CDM Learning Program

## Learning Community Event

**WHO:** IT Operations and Mgmt, IT Security

**WHAT**: Two-hour event to discuss information, share best practices

**WHERE:** DC Metro area and online

**WHEN:** 4th week of each month

**WHY:** To exchange knowledge, share experiences, create best practices, collaborate, and network

**HOW:** F-2-F, Virtual World, and HSIN Connect

**September 29**

Vulnerability Management: Lessons from the Field

**94% of participants agree "the material presented was timely and relevant to my work" (February 2016)**

# CDM Learning Program

## Online Vignettes

**WHO:** IT Operations and Mgmt, IT Security

**WHAT**: 3 – 8 minutes vignettes explaining CDM core concepts

**WHERE:** Online

**WHEN:** Anytime

**WHY:** Increase baseline knowledge of CDM concepts

**HOW:** FedVTE and SEI StepFwd platforms

FedVTE:
https://fedvte.usalearning.gov/

# CDM Learning Program

## Guides

**WHO:** IT Operations and Management, IT Security

**WHAT**: Training documents with useful recommendations on CDM program implementation and security capabilities

**WHERE:** Online

**WHEN:** Anytime

**WHY:** To help drive intra-agency awareness and solution adoption

**HOW:** CDM Learning Website: www.us-cert.gov/cdm

**Readiness & Planning Guide for Asset-Based CDM Security Capabilities**

**CDM Roles and Responsibilities**

# CDM Learning Program

## KEY TAKE AWAYS

- No external training costs
- Increased awareness and knowledge **=** increased motivation and enthusiasm for continuous monitoring, automating security control assessments, risk management, improving information system security….
- Supports Cyber National Action Plan

PREPARATION BEGINS WITH UNDERSTANDING

…..

**JOIN OUR MEMBERSHIP LIST:**

**cdmlearning@hq.dhs.gov**

**VIEW CONTENT AT:**

**www.US-CERT.gov/cdm**

# Questions and Answers

PREPARATION BEGINS WITH UNDERSTANDING

.....

# Thank You

JOIN OUR MEMBERSHIP LIST:
cdmlearning@hq.dhs.gov

VIEW CONTENT AT:
www.US-CERT.gov/cdm