Homeland Security

Talk with the Authors of NISTIR 8011
March 31, 2016
1:00 pm – 3:00 pm

A CDM Learning Community Event

The CDM Learning Program

CDM Learning Program – What's in it for you:

- Monthly Learning Community Event (CDM-LCE)
  - CDM leaders and implementers discuss relevant CDM topics in-depth, either in a live face-to-face session or using a virtual platform such as AvayaLive!
- Monthly Webinars
  - CDM experts deep-dive into specific CDM topics and participants are able to ask relevant questions using a text-chat function
- Weekly CDM Bits & Bytes
  - Short email awareness tips that link to additional content posted to the CDM Learning forum on GovLoop
- Online Vignettes
  - Short video vignettes which allow the learner to develop foundational knowledge around key CDM concepts and topics

Resources Available: https://www.us-cert.gov/cdm

Sign up to receive information on Learning Community Events
by emailing cdmlearning@hq.dhs.gov

Today's Agenda

- Welcome and overview of today's event
- Panelist introductions, opening remarks
- Moderated Q&A session – Talk with the Authors of NISTIR 8011
- Panelists closing comments
- Final remarks, conclusion

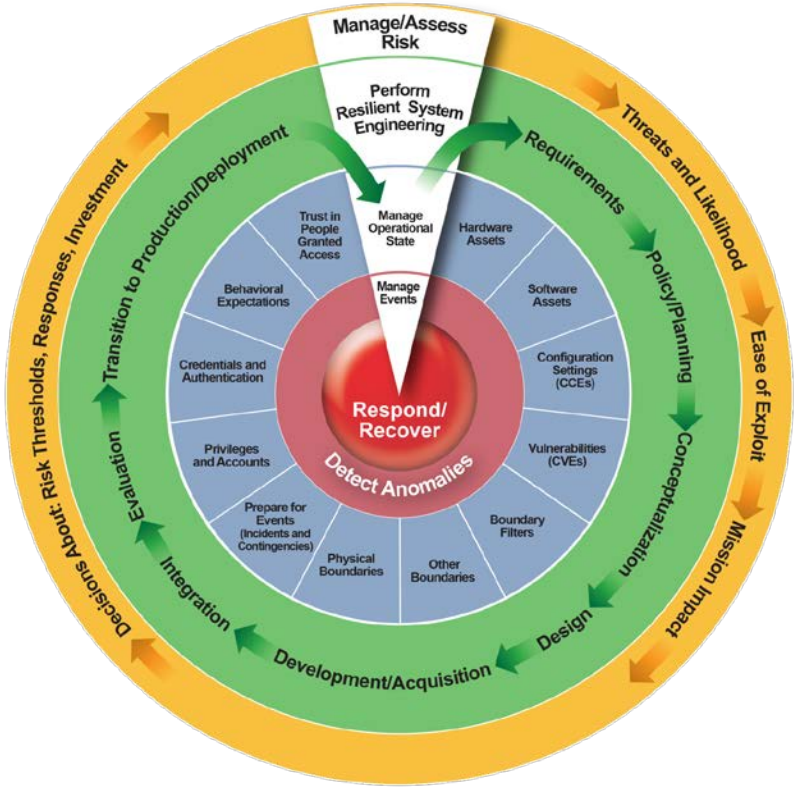
NISTIR 8011 Vol 1 and Vol 2
Automation Support for Security Control Assessment

Today's Panelists

Kelley Dempsey, NIST

Paul Eavy, DHS FNR

George Moore, JHU APL



Event Conclusion

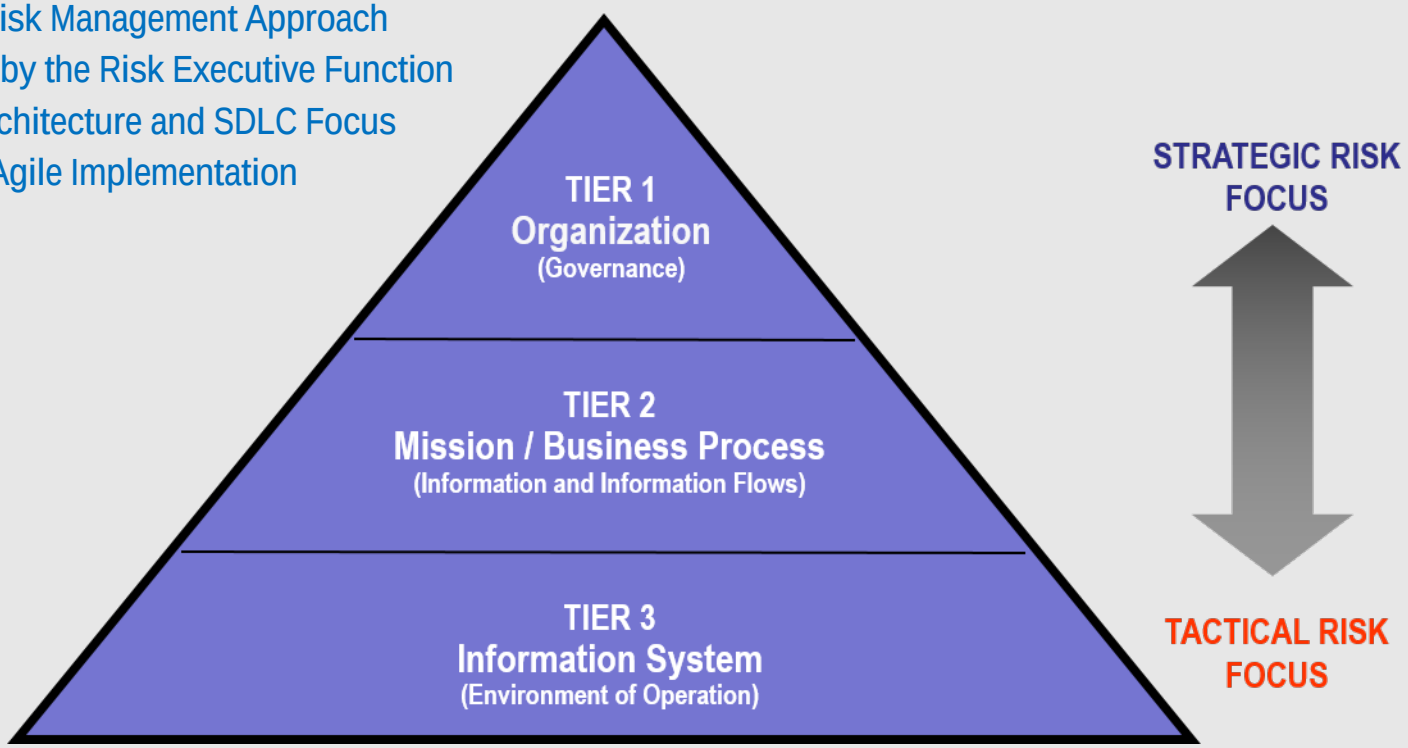
Thank you for attending today's CDM Learning Community Event!

- A certificate of attendance will be available to download on the CDM Learning Program website at www.us-cert.gov/cdm/training, within one week of today's event
- Visit our website to learn more about the CDM Learning Program and upcoming events at www.us-cert.gov/cdm
- For any questions or comments, please email us at www.cdmlearning@hq.dhs.gov

BACKUP SLIDES

Enterprise-Wide Risk Management

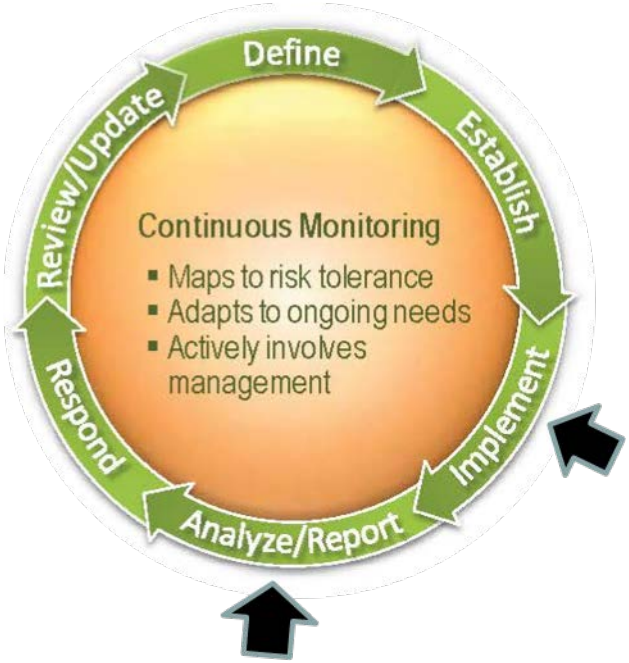
- Multi-tiered Risk Management Approach
- Implemented by the Risk Executive Function
- Enterprise Architecture and SDLC Focus
- Flexible and Agile Implementation



Source: NIST, SP 800-37

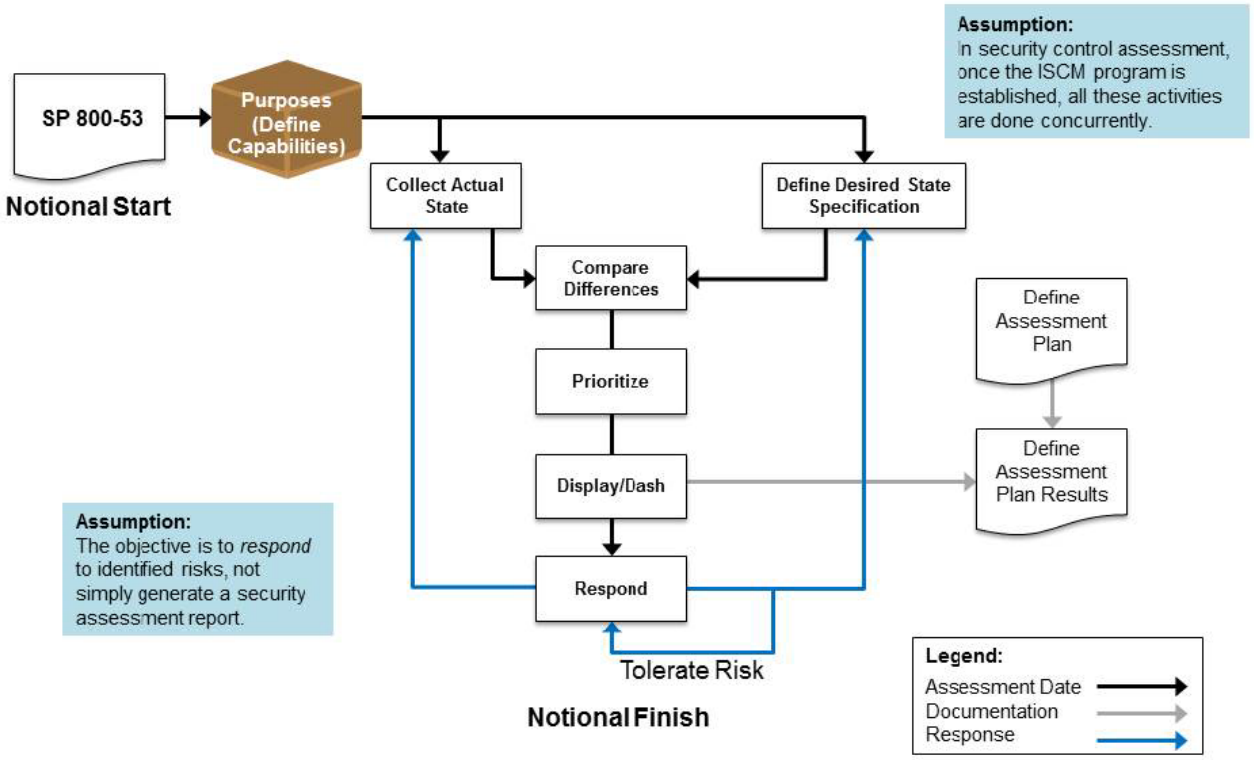
Linkage between Monitoring and Automated Assessment

NIST SP 800-137
Information Security Continuous Monitoring (ISCM) for Federal Systems and Organizations



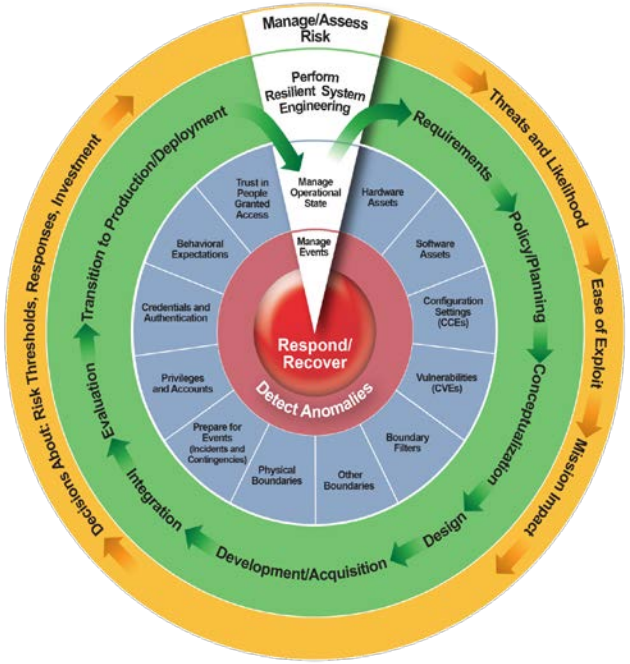
In the ISCM process, automated assessment encompasses the *Implement* and *Analyze and Report* steps.

Overview of the ISCM Ongoing Assessment Process



Source: NISTIR 8011, vol 1

ISCM Security Capabilities



ISCM Security Capabilities

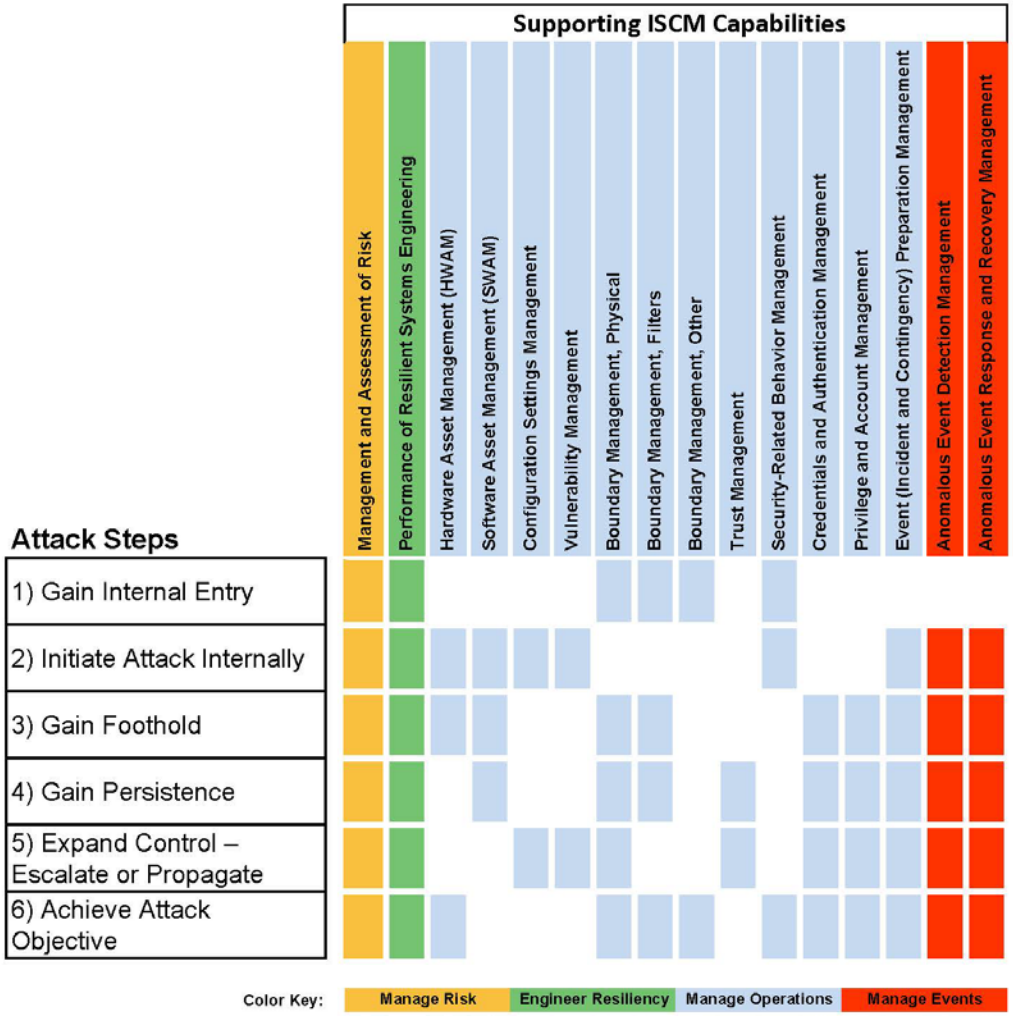
As suggested by SP 800-53A Rev 4, security *capabilities* are groups of security controls working together to support a particular *purpose*.

NISTIR 8011 Automation Support for Security Control Assessment

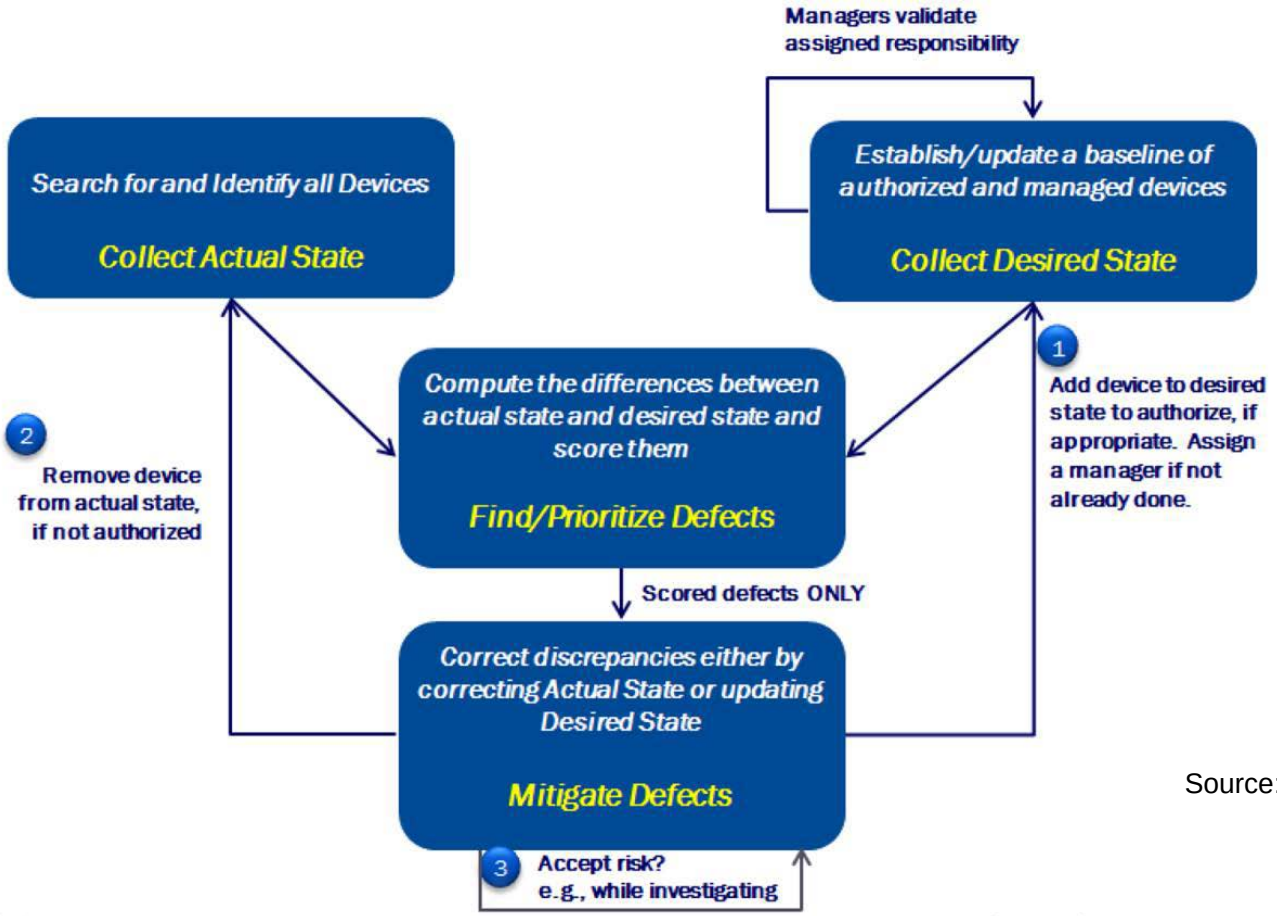
Defending Against Attack Steps

The common *purpose* of each security capability is to block or limit the damage from one or more step(s) of a cybersecurity attack.

ISCM Security Capabilities Defend Against Attack Steps



HWAM Concept of Operations



Source: NISTIR 8011, vol 2