

Continuous Diagnostics and Mitigation

Roles and Responsibilities Guide

Version 2.1

February 17, 2016



Homeland
Security

Federal Network Resilience

Revision/Change Record

Revision	Date	Revision/Change Description	Pages Affected
Version 1.0	June 4, 2015	Formal Draft	All
Version 2.0	October 14, 2015	Incorporate minor changes and change document name from “ <i>Governance Framework Roles and Responsibilities</i> ” to “ <i>Continuous Diagnostics and Mitigation: Roles and Responsibilities Guide</i> ”	All
Version 2.1	February 17, 2016	Published final version 2.1	All

Table of Contents

1	Purpose.....	4
2	Background.....	5
3	Guide Basics	6
3.1	Key Enablers of CDM Program Readiness and Implementation	6
3.2	Communications	7
3.2.1	Training.....	7
3.2.2	Workforce.....	7
3.2.3	Relationship to Other CDM Guides	7
4	Role and Responsibility Considerations for Adaptation.....	8
4.1	Chief Information Officer (CIO).....	8
4.1.1	Risk Executive (Function).....	8
4.1.2	Authorizing Official	9
4.2	Chief Information Security Officer (CISO)/Senior Information Security Officer (SISO) .	9
4.2.1	Information System Security Officer	9
4.2.2	Common Control Provider	9
4.2.3	Security Control Assessor	10
4.2.4	RMF Program Manager	10
4.2.5	ISCM and CDM Manager(s).....	10
4.2.6	Local Scoring and Metrics Group	11
4.3	Information System Owner (ISO)/Information Owner/Steward	11
4.3.1	D/A Help Desk	11
4.3.2	Mitigators	11
5	Conclusion	12
Appendix A:	References	13
Appendix B:	Program Resources.....	14
Appendix C:	Acronym List	15

CDM Roles and Responsibilities Guide

1 Purpose

This document proposes roles and responsibilities for organizations implementing the Continuous Diagnostics and Mitigation (CDM) program. It is intended to be used by Departments and Agencies (D/As) in coordination with their Continuous Monitoring as a Service (CMaaS) provider to integrate the roles and responsibilities from the CDM Program into the existing security management structures of their D/A.

This document is intended to provide guidance in two areas:

- how the CDM Program impacts decision-making within a D/A
- the roles and associated responsibilities of the stakeholders, enabling the CDM Program to be successfully implemented and managed within existing processes and procedures.

It is not intended to be a design or implementation framework, which is the responsibility of the CMaaS BPA Lead Provider.

DHS recognizes that organizations have different practices for managing information systems, depending on their mission; size; structure; nature, scope and complexity of operations; and risk profile.

This document does not mandate role and responsibility requirements within a D/A. The senior officials and managers of the D/A are responsible for creating requirements for implementing the management structure of the CDM. This guide assists the D/As by identifying the essential roles and responsibilities that form the basis of successful CDM Program deployment, operation, and maintenance. It is anticipated that D/As could utilize this information in alignment with the current structure of their information security management. DHS realizes that not all “roles” exist within a D/A, especially within small and micro agencies. Therefore, D/As are encouraged to customize the roles as appropriate.

2 Background

The CDM Program is a dynamic approach to fortify the cybersecurity of government networks and systems. It provides federal D/As with the capabilities and tools to conduct automated, on-going assessments. The CDM Program is coordinated by the Department of Homeland Security (DHS) to support all civilian sector federal departments and agencies. Congress established it to provide adequate, risk-based, and cost-effective cybersecurity assessments and more efficiently allocate cybersecurity resources.

The CDM Program enables Federal D/As to expand their continuous diagnostic capabilities by increasing the capacity of their network sensors, automating the collection of data from sensors, and prioritizing risk alerts. CDM offers a catalog of commercial off-the-shelf (COTS) tools, with the ability to update the catalog for technical modernization as threats change.

Many organizations use sensors to record the actual state of system configurations that affect security. The CDM Program enables the desired state specification to be expressed in data so that it can be easily compared to the system's actual state, highlighting differences. The results feed into a D/A dashboard that produces customized reports, alerting CDM managers and mitigators to their worst and most critical cyber risks. Prioritized alerts enable agencies to efficiently allocate resources based on the severity of the identified risk. Standard progress reports track results, which can be shared among organizations. Summary information feeds into component dashboards from the Federal level dashboard to inform and prioritize cyber risks.

For more information, please refer to the CDM Portal, hosted on the Homeland Security Information Network (HSIN), listed in the references section. In addition, more information can be found on the CDM webpage: <https://www.us-cert.gov/cdm>. You can contact the program office at cdm.fnr@dhs.gov.

3 Guide Basics

3.1 Key Enablers of CDM Program Readiness and Implementation

The effective execution of the CDM Program requires collaboration across multiple activities and time phases, 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 for participating departments/agencies
- Implementation: deployment of CDM sensors, services, and dashboards at participating departments/agencies
- Operations: operation of the sensors as well as management of the Federal CDM dashboard to identify, prioritize, and inform mitigation of and oversight of systemic cybersecurity risks

Each of these activities encompasses specific program management requirements. These requirements can be further clarified through the decomposition of program management as authority, decision-making, and accountability. Authority, in this context, can be defined as who (either an individual or organization) makes particular decisions essential to achieving program outcomes. Decision-making is the set of processes and associated information that contribute to a program decision and define or constrain a set of decision options. Accountability includes the methods through which various stakeholders are included in decision-making, the process and information used to evaluate the decision, and the methods of sharing such evaluation with stakeholders to inform future decisions.

Effective security management throughout the NIST SP 800-37 Risk Management Framework (RMF) tiered risk management approach (organization level, mission and business process level, and information system level) are dependencies for the success of the CDM Program. 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. In addition, security management processes and structures cannot remain static. Instead, they must evolve with and anticipate the trajectory of the CDM Program and adapt accordingly.

Effective and enduring security management structures and processes depend upon various enabling activities. These activities ensure that CDM roles and responsibilities are implemented effectively and in a standardized manner across various stakeholders.

3.2 Communications

Information sharing is the foundation that precedes and enables successful security management. Ongoing structured and ad hoc communications are required between various partners within and among the security management roles. In some cases, specific communications processes will be required. The need for such codified communication is exemplified by OMB Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*. It sets forth specific requirements for agency Information Security Continuous Monitoring (ISCM) programs that will in many cases be fulfilled by CDM acquisition, implementation, and operations.

3.2.1 Training

Effective security management of the CDM Program requires a common understanding of CDM concepts and principles. DHS is developing a training curriculum that will be available to all Federal D/As and, if applicable, their CMaaS supporting contractor.

3.2.2 Workforce

Closely allied with training is the need to define and promote the workforce associated with the CDM Program. CDM requires a fundamental shift in the federal cybersecurity workforce away from paper-based compliance to a focus on risk-based automated diagnostics and proactive mitigation. The need for a holistic workforce transition further provides an opportunity for DHS (and the US government more broadly) to promote the inclusion of operationally effective skills and knowledge into the curriculum of training and education programs.

3.2.3 Relationship to Other CDM Guides

The *Roles and Responsibilities Guide* proposes roles and responsibilities for D/As implementing the CDM security capabilities.

The *Readiness and Planning Guides* propose questions for D/As to consider before implementing CDM security capabilities.

The *Implementation Guides* describe the recommended operational practices for CDM security capabilities.

4 Role and Responsibility Considerations for Adaptation

This section identifies the responsibilities that D/As are encouraged to consider when implementing CDM within their organization. For consistency, the role titles are aligned with the roles in NIST Special Publication 800-37 Rev. 1. Multiple roles may be filled by one person. D/As are encouraged to adapt these roles as appropriate.

4.1 Chief Information Officer (CIO)

- Sponsor and promote the ISCM program within the D/A.
- Identify and assign representatives to federal-level ISCM scoring and metrics working groups as they evolve.
- Identify D/A and CIO-Level reporting requirements that are fulfilled by the CDM Program.
- Establish a no-fault scoring and grading phase of initial operations and determine when there is consensus of fairness and objectivity that justifies leaving the no-fault phase.
- Establish processes to ensure that federal and D/A dashboard results are used effectively to fix the worst problems first and to manage risk.
- Determine how to integrate the CDM guidance material into the organization's broader information security management structures and policies.
- Use the federal and D/A dashboard data to make information security investment decisions to address persistent issues.
- Ensure that CDM Program staff has the training and resources (e.g., staff and budget) needed to perform assigned duties.

In addition, the CIO has general oversight of the following functions:

4.1.1 Risk Executive (Function)¹

- Work with the ISCM/CDM Program Managers² to ensure reporting categories cover the three risk levels described in NIST SP 800-39: (i) organization level; (ii) mission/business process level; and (iii) information system level.
- Work with federal-level management bodies and ISCM/CDM program managers to ensure federal and D/A reporting categories cover risk scores.
- Coordinate with Authorizing Officials (AO), System Owners, and other authoritative sources of guidance on how to use CDM dashboard data for situational awareness and active risk management.

¹ The Risk Executive (Function) is defined in NIST SP 800-39 (2011) *Managing Information Security Risk Organization, Mission, and Information System View* Section 2.3.2: "The risk executive is a functional role established within organizations to provide a more comprehensive, organization-wide approach to risk management.

² See OMB M-14-03 (November 18, 2013) *Enhancing the Security of Federal Information and Information Systems*, all agencies are required to "Identify specific individuals to manage the agency ISCM program" (page 7).

- Establish triggers for unacceptable risk situations using CDM dashboard, and (implicitly) acceptable risk.

4.1.2 Authorizing Official

- Work with security managers to establish system-level reporting categories to be viewed in the D/A dashboard.
- Use data from the D/A dashboard to assess risk on an ongoing basis.

4.2 Chief Information Security Officer (CISO)/Senior Information Security Officer (SISO)

- Designate a qualified person to be responsible for CDM Program management and implementation.
- Identify CDM Program stakeholders and establish a process to keep them informed about the program.
- Identify FISMA and CISO-level reporting requirements that are fulfilled by the CDM Program.
- Use data from the federal and D/A dashboards to make information security investment decisions to address persistent issues.
- Establish triggers (i.e., indicators or prompts that cause the D/A to react in a predefined manner) for unacceptable risk situations using the D/A dashboard and (implicitly) acceptable risk.
- Ensure that CDM Program staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.

In addition, the CISO/SISO has general oversight of the following functions:

4.2.1 Information System Security Officer

- Work with appropriate security officials to establish appropriate reporting requirements at the system level.
- Use data from the D/A dashboard to assess risk on an ongoing basis.
- Use data from the D/A dashboard to make information security investment recommendations that address persistent issues.

4.2.2 Common Control Provider

- Work with appropriate security officials to establish appropriate reporting requirements that are fulfilled by the CDM Program at the common control level.³

³ U.S. Office of Management and Budget. *Enhancing the Security of Federal Information and Information Systems*. By Sylvia M. Burwell. Available at <https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>. Accessed: 8/19/2015.

- Use the D/A dashboard data to assess risk on an ongoing basis.

4.2.3 Security Control Assessor

- Establish appropriate reporting requirements in adherence to the NIST SP 800-37 RMF program for use in automated control assessment.
- Continue to use non-automated assessment methods where CDM data is not yet of adequate sufficiency or quality.

4.2.4 RMF Program Manager

- Develop processes with your Office of Inspector General (OIG) to share information regarding CDM and its impact to security control assessment.
- Identify reporting requirements for use in automated control assessment.
- Determine how CDM results will be used in ongoing authorization (refer to NIST Supplemental Guidance on Ongoing Authorization: Transitioning to Near Real-Time Risk Management, June 2014)

4.2.5 ISCM and CDM Manager(s)

- Sensor Performance Management—coordinate with CMaaS provider to ensure that the following issues are addressed:
 - sensor access authorizations (including through firewalls)
 - data completeness (including availability)
 - data timeliness
 - error rates (false positives and false negatives)
- Establish dashboard access control process and procedures.
- Ensure that dashboard access control is managed adequately.
- Establish coordination with D/A Help Desk; examples include
 - pre-scripted solutions for issues
 - escalation rules and procedures
- Establish a process to provide technical help to mitigators.
- Coordinate reporting requirements across various users.
- Establish responsibilities for supporting implementation of each capability (when appropriate) and ensuring that staff receives training (using, at a minimum, DHS CDM provided training).
- Ensure that CDM Program staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.
- In coordination with their contracting officers, continue to address CDM and CMaaS efficacy post contract.

4.2.6 Local Scoring and Metrics Group

- Establish a liaison with the federal scoring and metrics working group.
- Establish and operate a process to manage the introduction of new risk.
- Establish configuration settings issues and coordination sub-group.
- Establish requirements for measuring and managing sensor performance.
- Establish and operate a process to implement risk transfers, such as creating a risk transfer sub-group.
- Manage risk scoring to include
 - decisions on how risk scores will be managed and how deviations from baseline settings are to be addressed
 - decisions on how local scores will be adjusted from the federal scoring/grading (or not)
 - validation and maintenance of fairness, transparency, reliability, and objectivity of scores
 - using scores and grades to motivate and assess performance while addressing concerns

4.3 Information System Owner (ISO)/Information Owner/Steward

- Work with appropriate security officials (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements at the system level.
- Use data from the D/A dashboard to assess risk on an ongoing basis.
- Use data from the D/A dashboard to make information security investment decisions that address persistent issues.
- Ensure that CDM Program staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.

In addition, the ISO has general oversight of the following functions:

4.3.1 D/A Help Desk

- As assigned, respond to CDM issues, escalate and coordinate.

4.3.2 Mitigators

- Review defect checks and mitigate risks on a timely basis.

5 Conclusion

These CDM roles and responsibilities provide initial guidelines for D/As to facilitate CDM deployment within their respective agencies and will be revised as the program develops.

Comments can be sent to the CDM Program office at cdm.fnr@dhs.gov.

Appendix A: References

NIST Publications: <http://csrc.nist.gov/publications/PubsSPs.html>, including

- NIST Special Publication 800-37 Rev. 1 (Feb 2010), *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r1.pdf>
- NIST Special Publication 800-39 (Mar 2011), *Managing Information Security Risk Organization, Mission, and Information System View*, <http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf>
- NIST Special Publication 800-53 Rev. 4 (Apr 2014), *Security and Privacy Controls for Federal Information Systems and Organizations*, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>
- NIST Special Publication 800-53A Rev. 4 (Dec 2014), *Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Assessment Plans*, <http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf>
- NIST Special Publication 800-55 Rev. 1 (Jul 2008), *Performance Measurement Guide for Information Security*, <http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf>
- NIST Special Publication 800-100 (Oct 2006), *Information Security Handbook: A Guide for Managers*, <http://csrc.nist.gov/publications/nistpubs/800-100/SP800-100-Mar07-2007.pdf>
- NIST Special Publication 800-137 (Sep 2011), *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, <http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>

Office of Management and Budget (OMB) Memorandum 14-03, *Enhancing the Security of Federal Information and Information Systems*, November 18, 2013

<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>

Olzak, Tim. "COBIT 5 for information security: The underlying principles." TechRepublic. September 4, 2013. <http://www.techrepublic.com/blog/it-security/cobit-5-for-information-security-the-underlying-principles/>

Appendix B: Program Resources

- US-CERT CDM: <http://www.us-cert.gov/cdm>
 - DHS CDM: <http://www.dhs.gov/cdm>
 - Homeland Security Information Network (HSIN):
<https://hsin.dhs.gov/dhs/CDM/Pages/Home.aspx>
(This web site contains training and portal pages for technical working groups. For access and other information, see contract staff.)
 - CDM Program contact information: cdm.fnr@hq.dhs.gov
 - GSA CDM: www.gsa.gov/cdm, or contact cdm@gsa.gov
- OMB Circulars and Memorandums:
http://www.whitehouse.gov/omb/memoranda_default

Appendix C: Acronym List

ACRONYM	DEFINITION
AO	Authorizing Officer
BPA	Blanket Purchase Agreement
CDM	Continuous Diagnostics and Mitigation
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMaaS	Continuous Monitoring as a Service
COTS	Commercial-off-the-Shelf
D/As	Departments and Agencies
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
GSA	General Services Administration
HSIN	Homeland Security Information Network
ISCM	Information Security Continuous Monitoring
ISO	Information System Owner
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OMB	Office of Management and Budget
RMF	Risk Management Framework
SISO	Senior Information Security Officer