Homeland Security

Continuous Diagnostics and Mitigation (CDM)

Technical Capabilities

Volume One

Defining Actual and Desired States

Version 1.1

July 18, 2017

Table of Contents

REVISION SUMMARY

Table of Changes

Version Number	Date	Revised by	Section
1.0	4/25/2017	CDM PMO	All
1.1	7/14/2017	CDM PMO	Reflecting edits from USDA, DOI and NIST

Introduction

Strengthening the security posture of Federal networks, systems, and data is one of the most important challenges we face as a nation. Therefore, the Department of Homeland Security (DHS) seeks to provide agencies with the Continuous Diagnostics and Mitigation (CDM) Program to safeguard, secure, and strengthen cyberspace and the security posture of Federal networks in an environment where cyber attacks are continuously growing and evolving.

The CDM Architecture Principles document defines defect checks as “automated tests that compare an object’s actual state (as derived from sensors) with the desired security state (as established by policy).”

This document discusses how agencies can define the desired state within the CDM program, leveraging three frameworks: that of the CDM architecture (ABCD diagram), the Cybersecurity Framework, and the security controls framework outlined by the National Institute of Standards and Technology (NIST).

Since the cybersecurity space is inherently complex, the CDM approach is to address the problem space in phases, as shown in Figure *1*:

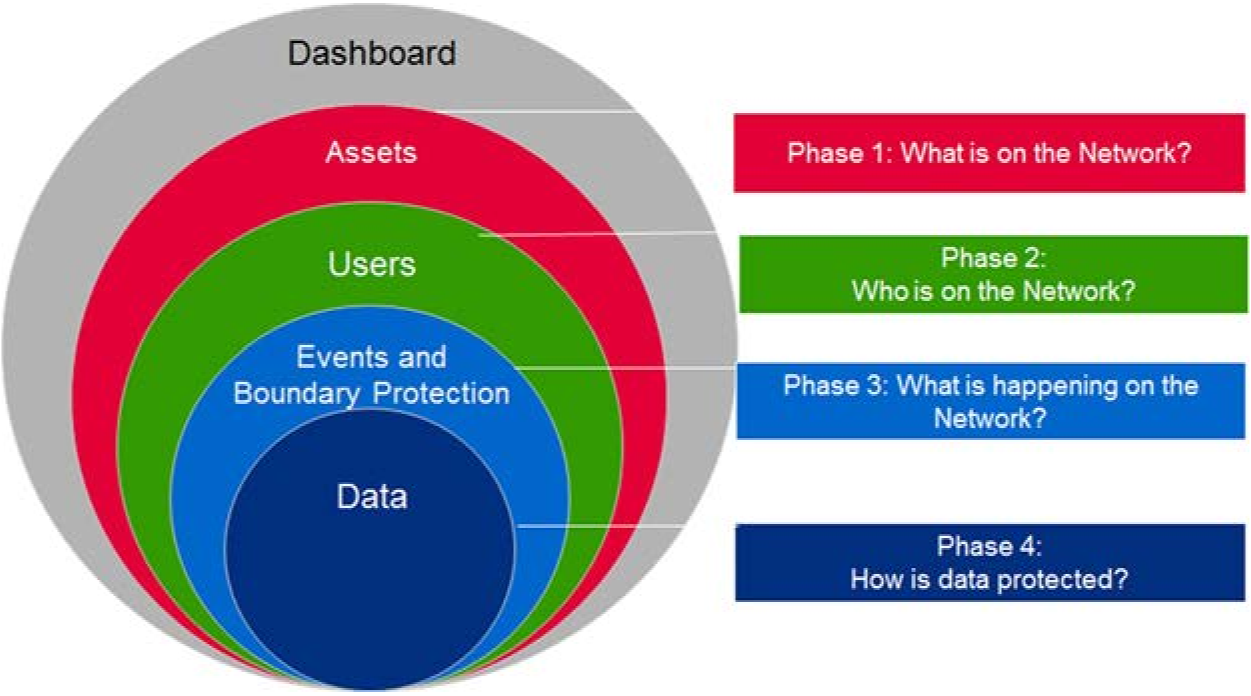

Dashboard
Assets
Users
Events and Boundary Protection
Data
Phase 1: What is on the Network?
Phase 2: Who is on the Network?
Phase 3: What is happening on the Network?
Phase 4: How is data protected?

Figure 1-Phases of CDM

NOTE: While Phase 4 is recognized as part of the CDM overall program, this document will focus on Phases 1, 2 and 3, for which there are defined requirements. It is expected that there will be an update to this document as the Phase 4 requirements are defined.

The guiding principle of the CDM approach is to observe the “actual state” of the components that form the network, have a targeted “desired state” match to the Agency’s abilities, and provide the mechanism to implement the improvement, usually through the removal of security "defects," with accompanying performance metrics to demonstrate the "value" of the improvement—often risk reduction.

It is important to note that while the scope of this document is the portion of the CDM program that is deployed within Agency environments, limitations of funding and other considerations will determine the prioritization and scoping of the breadth and depth of solutions deployed.

From the viewpoint of requirements, the CDM solution is composed of two distinct elements. The first is the CDM Dashboard (both Federal and Agency specific); the second is the collection of elements that are not in the scope of the Dashboard. The latter are labeled the Continuous Monitoring as a Service (CMaaS) elements and are the basis for the requirements captured in the companion volume (Volume Two), "CDM Technical Capabilities – Requirements Catalog." The Dashboard follows its own requirements process in alignment with the use of the agile methodology.

This document addresses the security frameworks supported by CDM and presents the major approaches applied to the definition of security posture and how each identifies the desired state. The Agency-defined "desired state" can take on different values depending on the security framework selected. Under this approach, the following are addressed:

1. The CDM-centric solution architecture and related constructs
2. CDM and the NIST Cybersecurity Framework
3. CDM and NIST Risk Management Framework, focused on the relationship of the NIST Special Publication (SP) 800-53 controls
4. CDM as defined through the compendium of capability requirements known as "Attachment Ns"

Security Frameworks Supported by CDM

The ability of an Agency to identify and implement correct security safeguards depends on its processes and procedures to assess, manage, and improve its security posture. Different approaches are often used to implement, assess, and evaluate the current state of security posture against Agency security goals, and to provide measurable guidelines for selecting appropriate security improvements. The lens by which Agencies select the desired state provides different contextual boundaries against which a given object as may be represented through these security frameworks.

This section outlines how leveraging the CDM architecture (including CDM design concepts), the NIST Cybersecurity Framework, and the NIST Risk Management Framework (with emphasis on the NIST SP 800-53 controls) can provide a measurable CDM approach to assess and improve an Agency's information system security posture.

I - 1 CDM Architecture

This approach looks for conformance to the CDM architecture as a reference framework. The approach includes both the conceptual CDM architecture and the associated core design concepts.

I - 1.1 CDM ABCD Architecture

The CDM architecture uses a four-layer A-B-C-D design, as shown in Figure 2-ABCD Notional Architecture. Since the requirements for Phase 4 are in process, only Phases 1, 2, and 3 are shown.

- Layer A is the lowest and most diverse layer, containing tools and sensors that are deployed and interact with the low-level hardware and software components in an Agency's information system infrastructure. Almost by definition, Layer A is highly distributed and rarely centralized.
- Layer B serves as the contractor integration point specific to the Agency-provided solution. It is dual purposed, supporting the data integration and normalization function as well as orchestrating the operational control points for the CMaaS solution. The subsystems that form Layer B may be centralized but should be able to accommodate horizontal or vertical implementation either for scaling or geopolitical reasons. The general recommendation (at minimum) is that the instances of Layer B should align to the topology employed for Layer C.
- Layer C is the Agency Dashboard provided as government-furnished equipment by the CDM program to the contractor to customize as appropriate for the Agency environment. It is the Agency's exclusive (authoritative) connection to the Federal Dashboard and receives its Agency feeds from Level B. The inherent structure of the agency Dashboard supports a hierarchical implementation to accommodate horizontal or vertical implementation either for scaling or geopolitical reasons.
- Layer D provides dashboards and repositories at the Federal Enterprise level. The Federal level holds the Agency summary material and provides the standards and policies feed to the Agency Dashboards. As such, this area has no CMaaS contractor responsibilities and is being provided by a separate CDM Dashboard Task Order.

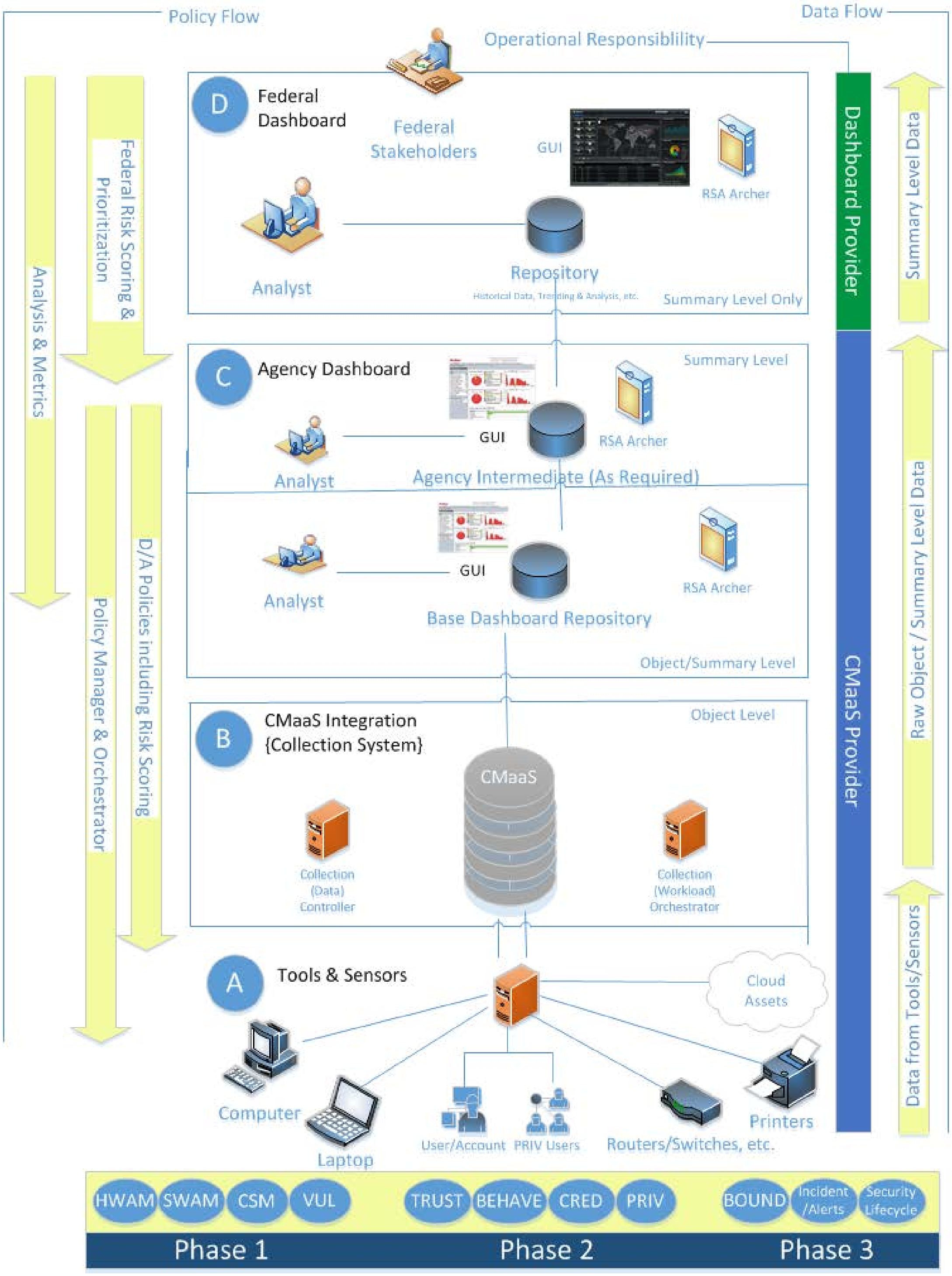


Figure 2-ABCD Notional Architecture (Phases 1 through 3)

To compute an Agency security risk, CDM monitors and collects hardware and software component actual state data values in Layer A. These values represent the actual state of an Agency's information system security posture. Layer B aggregates and correlates the actual state data values for evaluation against the desired state policy data, and through the Layer B orchestration desired state parameters (such as Organizational Unit [OU] or Federal Information Security Modernization Act 2014 [FISMA] structures) can be passed to and executed by Layer A.

While data collection is an upward flow, CDM Federal and Agency desired state policies flow from Layer D and Layer C, respectively. These policies are used to establish the desired state of an Agency information security posture based on the threats facing the Agency.

The risk scores, security risk, and gaps between the desired and actual states are reported to the Federal and Agency Dashboards for further analysis and actions. To address a security risk or lower a risk score, additional Federal or Agency desired state policies may be sent to augment existing security controls to mitigate the security risk.

I - 1.2 CDM Requirements Core Design Concepts

The core design concepts in this section are applicable to implementing CDM requirements in terms of desired and actual state processing:

- CDM Actual State (section I - 1.2.1) represents the “as-is” state of an Agency’s current security posture.
- CDM Desired State (section I - 1.2.2) represents the “to-be” state for an Agency’s projected security posture.
- CDM Policy Decision Point Machine-Readable Policies (section I - 1.2.3) is the technique used to translate and maintain security policies that are used for ongoing assessment.
- CDM Containers and Objects (section I - 1.2.4) represent the categorization of security related data types and information to manage, control and maintain desired and actual state data values.

All the previously mentioned CDM design concepts must adhere to the following set of CDM architectural principles:

- *Data Interrogation Actions: The CDM system provides methods for users to interact with CDM data to support higher level security activities*.
- *Common Schema: The CDM system uses a common schema to ensure that all data made available for diagnostics in CDM is consistent across all participating agencies.*
- *Machine-Readable Policy: Federal and Agency policy is captured such that the CDM system can automatically compare that policy information to sensor information to determine defects.*
- *Risk Scores: The CDM system uses risk scores to prioritize defects.*
- *Result Data Types: The CDM system provides different result data types to support various reporting needs within the CDM architecture layers.*
- *Grouping Object Data: The CDM system provides the ability to group object data to provide context to results and support security and authorization decisions.*

I - 1.2.1 CDM Actual State

The CDM actual state is the discoverable, observable, and measurable state of the security attributes associated with the relevant containers and objects that are generated from sensor hardware and software components. The relevant security information to be measured for containers, objects, and attributes is determined based on the needs of the NIST SP 800-53 controls (or additional organizationally defined security controls) and other security oversight sources, such as FISMA, and others as may be identified by the Office of Management and Budget (OMB) Circulars such as A-130. The actual state includes the states and behaviors (reflected in attribute values) that may indicate the presence of a change in security posture that may introduce additional risk to the information system.

In relationship to the CDM architecture, CDM actual state values are collected and generated in Layers A and B, respectively.

I - 1.2.2 CDM Desired State

The CDM desired state defines data values that represent the targeted best status of an Agency security posture. These data values may be in the form of an attribute with a specific value, a list of acceptable values, or a rule specification that includes desired values of other attributes. Rules for desired state attribute values may include attributes from containers and/or other objects. These rules can be used to build simple to complex relationships between different desired status attributes.

In relationship to the CDM architecture, CDM desired state policies are pushed down from Layers C and D and are very closely related to the Policy Decision Point operations defined below.

“Desired State” is continuously evolving, as a mature information technology (IT) governance process at the Federal level will contribute to identifying and approving the desired state attributes to protect the Agency information system.

I - 1.2.3 CDM Policy Decision Point Machine-Readable Policies

The CDM Policy Decision Point (PDP) is a logical mechanism used to measure the actual state against the desired state criteria.

The CDM PDP provides assurance that each information system component is configured with the correct policy (i.e., the desired state). The CDM PDP compares desired state attribute values with actual state attribute values using the policy and rules associated with that desired state. A discrepancy between a desired state attribute value and an actual attribute value (also known as a defect) represents a change in security posture for the information system. The change in security posture may be acceptable if the change in information system risk is acceptable. At this point, a policy decision is made to accept or mitigate the defect.

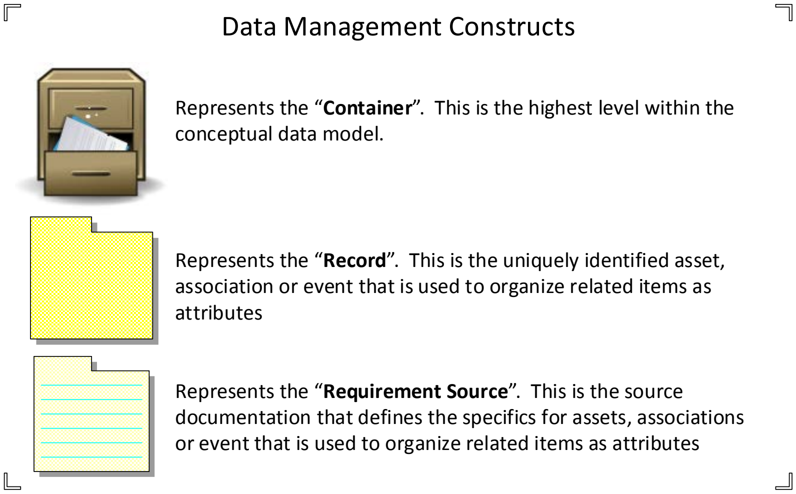
The CDM PDP supports the continuous monitoring of policies and attributes, and identifies and reports on policy discrepancies for an information system. To ensure that the ongoing assessment is automated, policies should be implemented in a machine-readable format that can be loaded into the CDM PDP.

To be machine readable, the CDM desired state policies must be expressed in a format that can be read and processed by the CDM PDP. That is, CDM attributes should be defined as values and lists that, when combined with rules, can be used to compute and measure the CDM ongoing assessment of the information systems to determine the ongoing authorization (see section I - 3.2) of the information system.

I - 1.2.4 CDM Containers and Objects

This section describes CDM containers and objects, graphically represented in the Figure 3, with the three key constructs being container, record, and requirement source.

The overall purpose of the CDM containers and objects is to store the results from the monitoring for state and behavior changes that impact the ongoing security risk level of information systems. This ongoing risk assessment and corresponding ongoing authorization will allow the determination whether information systems will be allowed to continue operations.



Represents the "**Container**". This is the highest level within the conceptual data model.

Represents the "**Record**". This is the uniquely identified asset, association or event that is used to organize related items as attributes

Represents the "**Requirement Source**". This is the source documentation that defines the specifics for assets, associations or event that is used to organize related items as attributes

Figure 3-CDM Data Model Legend

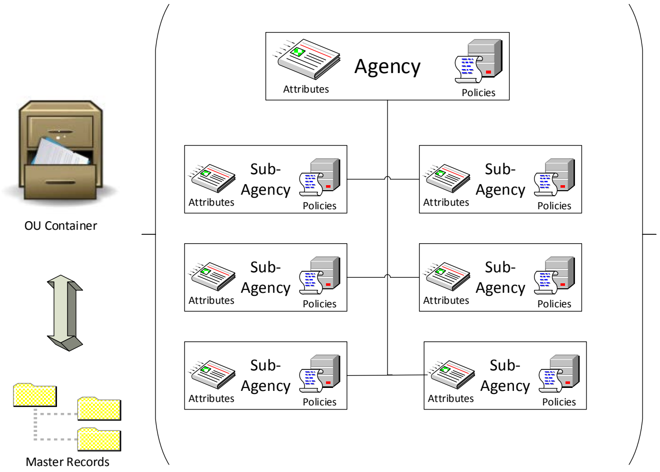
I - 1.2.4.1 Containers

CDM containers are the highest level of logical abstraction. CDM containers define the CDM policies and attributes for a given organization and system. There are two types of CDM containers: the OU Container (for example, under DHS, OUs might include components such as Immigration and Customs Enforcement, Customs and Border Protection, etc.) is used for organization-specific policies and attributes, while the FISMA Container is used for security policies and attributes that are required for compliance with FISMA.

The policies in a container specify values for attributes, relationships between object attributes (of potentially more than one object type), relationships between container attributes and object attributes, and/or a combination of these, for the CDM actual state and the CDM desired state. For example, the container may specify policies and attribute values for users of a device linked to the container.

I - 1.2.4.1.1 Organizational Unit Container

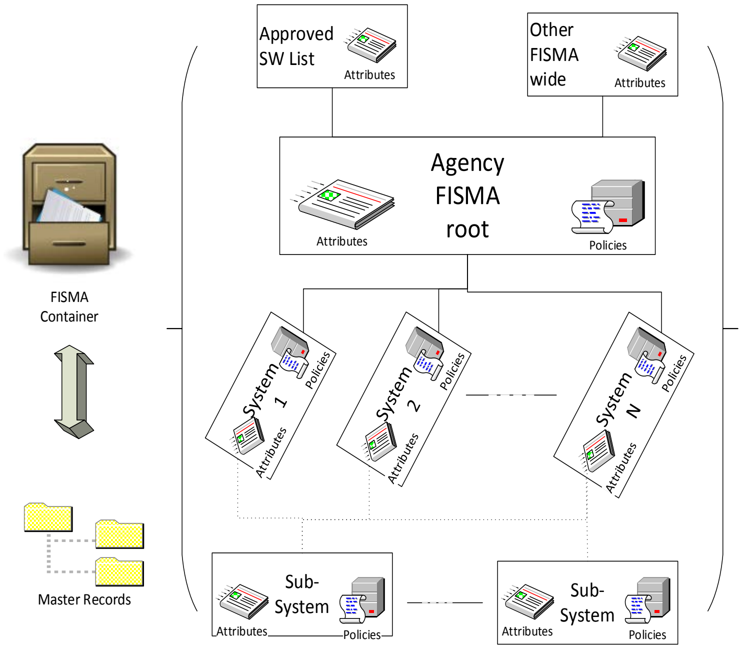
The OU Container is a set of policies and attributes that are applicable to information systems and users within the organization (e.g., an Agency). OU Containers represent the official organizational hierarchy. Attributes in the OU Container represent the organizational and functional roles (e.g., department heads, managers, etc.) and chain of command for the organization. The OU Container contains attributes for both the desired state and corresponding actual state for NIST SP 800-53 controls (or additional organizationally defined security controls) implemented at the organizational level, as well as other items required for reporting purposes.



The OU Container is composed of desired state policies and attribute values for attributes contained within various Master Records, which are compilations of attributes for the specified object (e.g., the Master User Record [MUR] for users and accounts, Master Device Record [MDR] for devices, Master System Record [MSR] for network interfaces, and/or Master Incident Record [MIR] for incidents and events) linked to the OU Container. These Master Records are described below.

I - 1.2.4.1.2 FISMA Container

The FISMA Container represents the authorization boundary for an information system, which defines the network, devices, and users that are part of the information system. The FISMA Container defines the security/mission assurance environment (e.g., data sensitivity, impact level, etc.) of the information system. Attributes in the FISMA Container represent the FISMA security roles (e.g., Risk Executive, Authorizing Official, Security Control Assessor, etc.), as well as security access roles (e.g., privileged and non-privileged users) for the information system. The FISMA Container contains attributes for both the desired state and corresponding actual state for NIST SP 800-53 controls (or additional organizationally defined security controls) implemented at the information system level, as well as other items required for reporting purposes.



The FISMA Container is composed of desired state policies and attribute values for attributes contained within the MUR, MDR, MSR, and/or MIR linked to the FISMA Container.

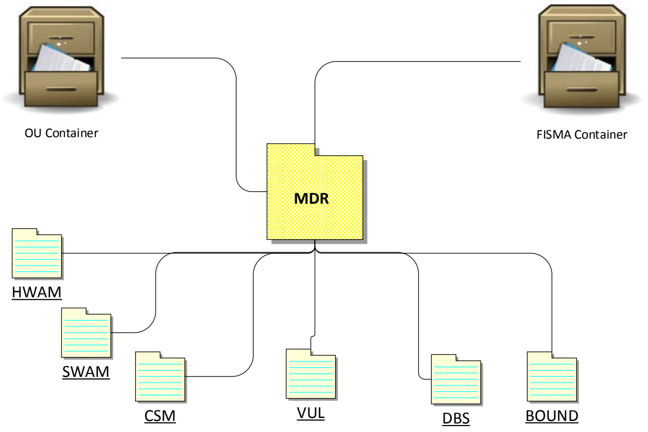
Controls implemented at the FISMA system level are linked to all systems and system components of the FISMA system associated with the FISMA Container. Further, the FISMA container can be used to hold enterprise control items such as the Approved Software List.

I - 1.2.4.2 Objects

Policies and attributes are derived and represented in CDM objects to capture instantiated actual attribute values during deployed runtime processing of information system components. CDM objects include the MDR, MUR, MSR, and MIR. These objects are associated with one or more OU Containers (based on the organizational hierarchy) and one or more FISMA Containers.

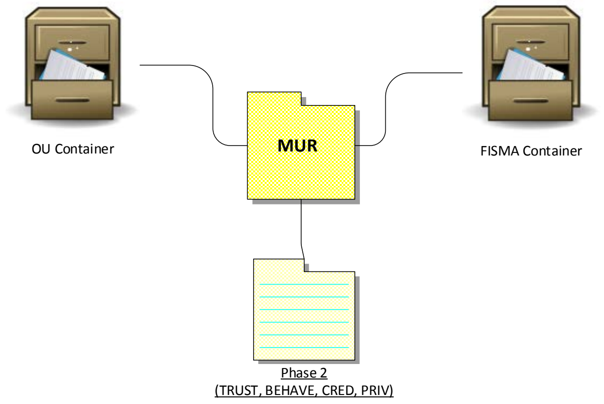
I - 1.2.4.2.1 Master Device Record

The MDR represents a physical or logical network device and deals with "What is on the network?" The MDR represents Internet Protocol addressable devices (e.g., router, switch, computers, mobile devices, etc.) and can include information about hardware, operating systems, installed applications, software services, connected devices (e.g., printers, universal serial bus [USB] devices, etc.), and hardware/software component configuration settings. The MDR contains attributes that need to be collected for comparison against a desired state for those attributes. The MDR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) to which the device belongs (i.e., is linked to). An MDR is linked to a single FISMA Container and may be linked to multiple OU Containers.



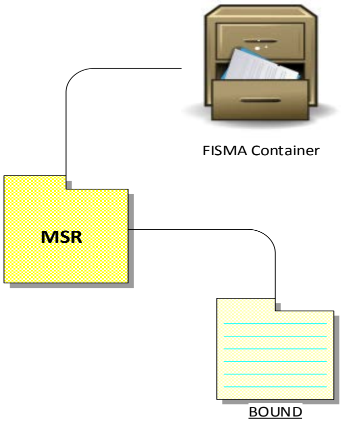
I - 1.2.4.2.2 Master User Record

The MUR represents an entity (person or non-person) that requests access to information, information systems, and facilities and deals with "Who is on the network?" The MUR includes information about credentials (i.e., elements of who) for identification, authorization (i.e., elements of trust) for access rights and permissions for granted access, accounts associated with information systems, and appropriate training for specific roles and responsibilities. The MUR contains attributes that need to be collected for comparison against a desired state for those attributes. The MUR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) linked to the item the entity is attempting to access. A MUR may be linked to multiple OU and FISMA Containers.



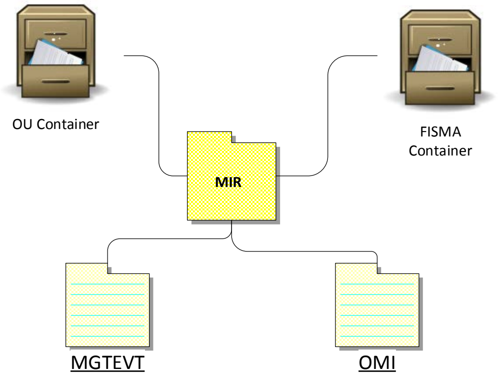
I - 1.2.4.2.3 Master System Record

The MSR represents the communication interface between information systems and deals with “How is the boundary protected?” The communication interface could be between information systems internal to the organization or with an information system external to the organization. The MSR contains attributes that need to be collected for comparison against a desired state for those attributes. The attributes are associated with one or more devices (MDRs) that mediate network traffic flow across the boundary (e.g., router, firewall, etc.) of the information system to implement the appropriate filtering policy. The MSR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) to which the information system belongs (i.e., is linked to). An MSR can be linked to multiple MDRs within the FISMA Container.



I - 1.2.4.2.4 Master Incident Record

The MIR represents activities associated with security controls that require an action when an event occurs and deals with “What is happening on the network?” The MIR includes information about the incident and the activities (e.g., Standard Operating Procedures, response/mitigation actions, reporting, etc.) associated with the incident. The MIR contains attributes that need to be collected for comparison against a desired state for those attributes. The MIR desired state is based on desired state policies and attribute values associated with the organization (OU Container) and/or FISMA system (FISMA Container) linked to the MSR, MDR, and/or MUR involved in the incident. An MIR may be linked to multiple OU and FISMA Containers, depending on the objects involved in the incident.



I - 1.2.4.3 Recap of Container/Objects

Figure 4 presents the container(s) and object(s) in a unified view of the entire conceptual data model.

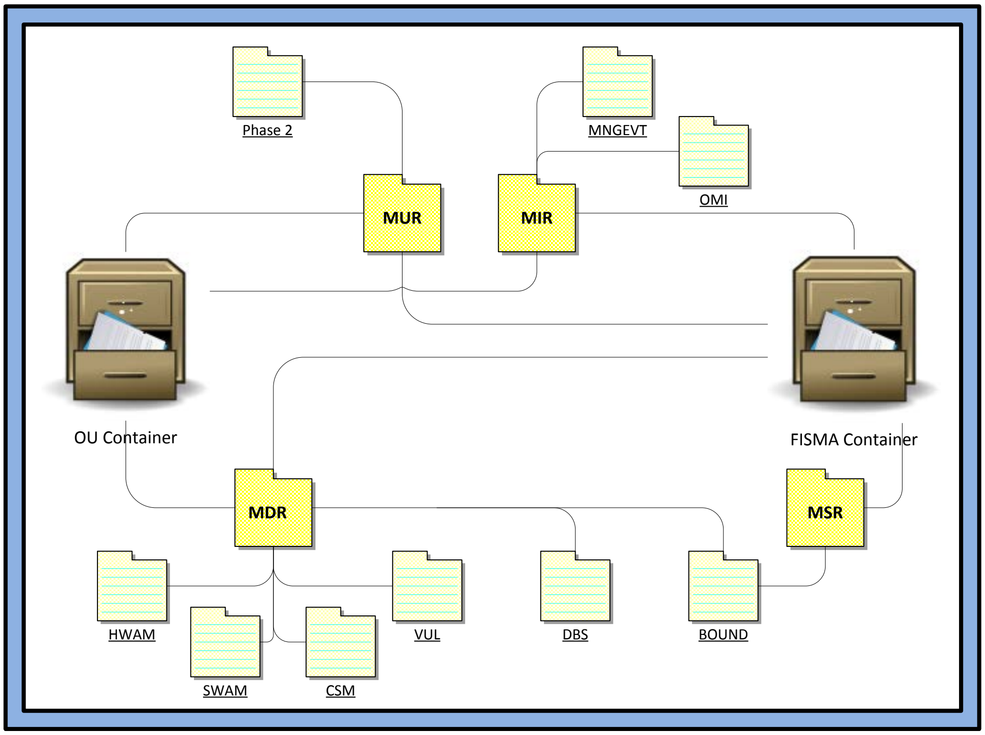


Figure 4-CDM Desired State Objects Relationship

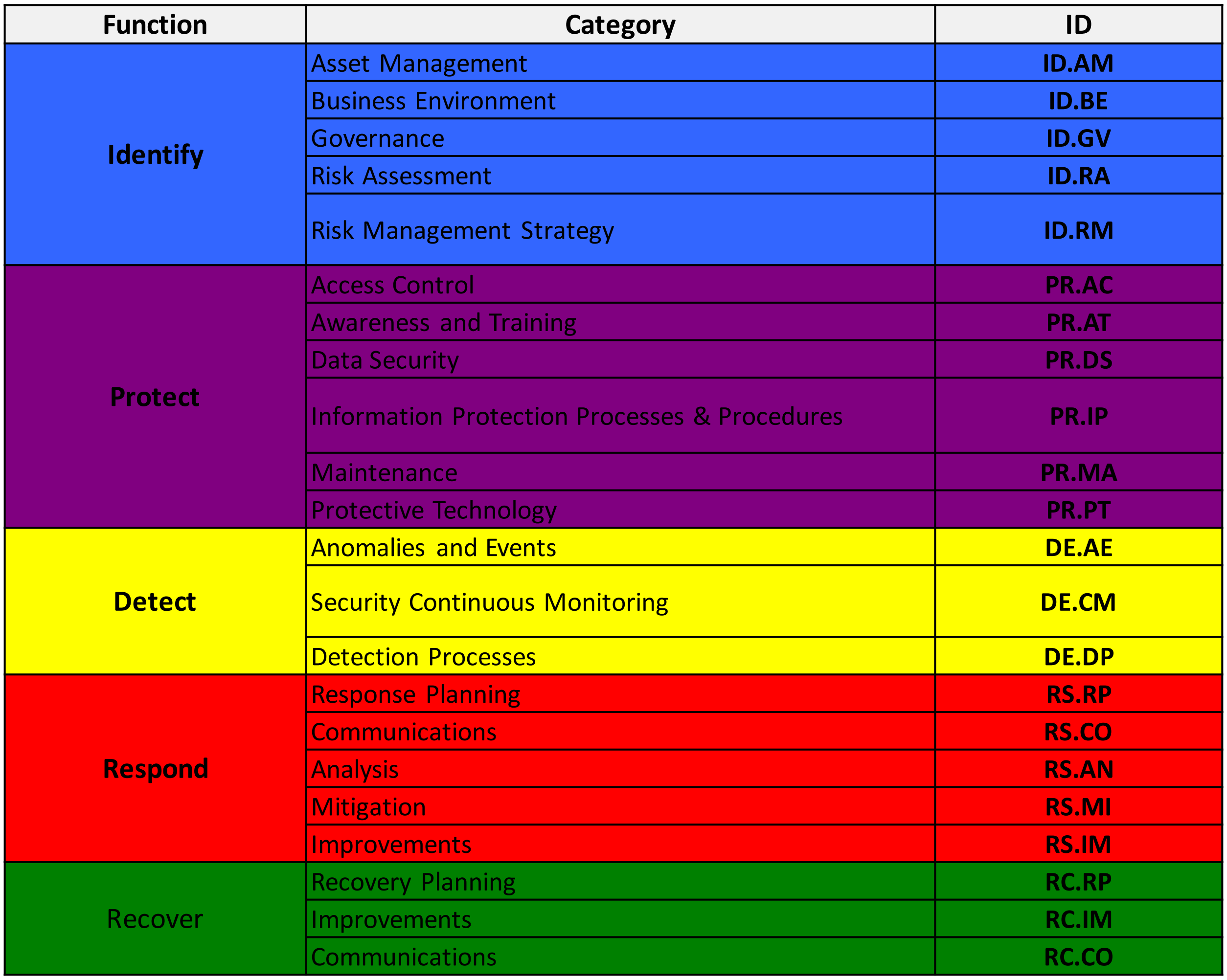
I - 2 CDM and the Cybersecurity Framework Core

OMB Memorandum 16-03, “Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,” calls out the Federal adoption of the NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.

The ability of an Agency to identify and implement correct security controls depends on its processes and procedures to assess, manage, and improve its security posture. To support that effort, security models are often used to continuously assess and evaluate the actual state of an Agency security posture against its desired state, and to provide measurable guidelines for selecting appropriate security improvements.

The NIST CSF Core comprises four elements: Functions, Categories, Subcategories, and Informative References. Currently, there are five Functions, 23 Categories (with IDs), and 98 Subcategories. This document covers only the CSF Core Functions and Categories with the Category ID in the third column (see Table 1) and shows how CDM tools, sensors, dashboards, and policies support the outcomes. The complete list of Categories to Subcategories mapping, and Subcategories mapping to Informative References, can be found in the NIST document *Framework for Improving Critical Infrastructure Cybersecurity*.

While the CDM program provides tools that meet the CDM goals and objectives to strengthen cybersecurity posture by continuous mitigation and diagnostics of security settings, it is not funded to procure cyber tools per se, but rather to provide tools that help agencies ensure that the cyber tools they do possess are appropriately configured.



Function	Category	ID
Identify	Asset Management	**ID.AM**
	Business Environment	**ID.BE**
	Governance	**ID.GV**
	Risk Assessment	**ID.RA**
	Risk Management Strategy	**ID.RM**
Protect	Access Control	**PR.AC**
	Awareness and Training	**PR.AT**
	Data Security	**PR.DS**
	Information Protection Processes & Procedures	**PR.IP**
	Maintenance	**PR.MA**
	Protective Technology	**PR.PT**
Detect	Anomalies and Events	**DE.AE**
	Security Continuous Monitoring	**DE.CM**
	Detection Processes	**DE.DP**
Respond	Response Planning	**RS.RP**
	Communications	**RS.CO**
	Analysis	**RS.AN**
	Mitigation	**RS.MI**
	Improvements	**RS.IM**
Recover	Recovery Planning	**RC.RP**
	Improvements	**RC.IM**
	Communications	**RC.CO**

Table 1: Cybersecurity Framework Core Element mapping

CSF defines Functions and Categories as follows:

- *Functions organize basic cybersecurity activities at their highest level. These Functions are Identify, Protect, Detect, Respond, and Recover. They aid an organization in expressing its management of cybersecurity risk by organizing information, enabling risk management decisions, addressing threats, and improving by learning from previous activities. The Functions also align with existing methodologies for incident management and help show the impact of investments in cybersecurity. For example, investments in planning and exercises support timely response and recovery actions, resulting in reduced impact to the delivery of services.*
- *Categories are the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities. Examples of Categories include "Asset Management," "Access Control," and "Detection Processes."*

Within the CDM program, the five CSF Functions are defined as follows:

Identify – What processes and assets need protection? Examples include identifying hardware assets, software assets, and vulnerabilities.

Protect – What safeguards are available? Examples include controls to protect and prevent compromise.

Detect – What techniques can identify incidents? Examples include monitoring to detect events and incidents related to vulnerabilities and weaknesses.

Respond – What techniques can contain impacts of incidents? Examples include identifying appropriate actions regarding detected cybersecurity events and incidents.

Recover – What techniques can restore capabilities? Examples include identifying plans for resiliency and to restore operational functions.

Descriptions of the 23 CSF Categories are shown in Section ***III - Appendix B: Cybersecurity Framework Categories.***

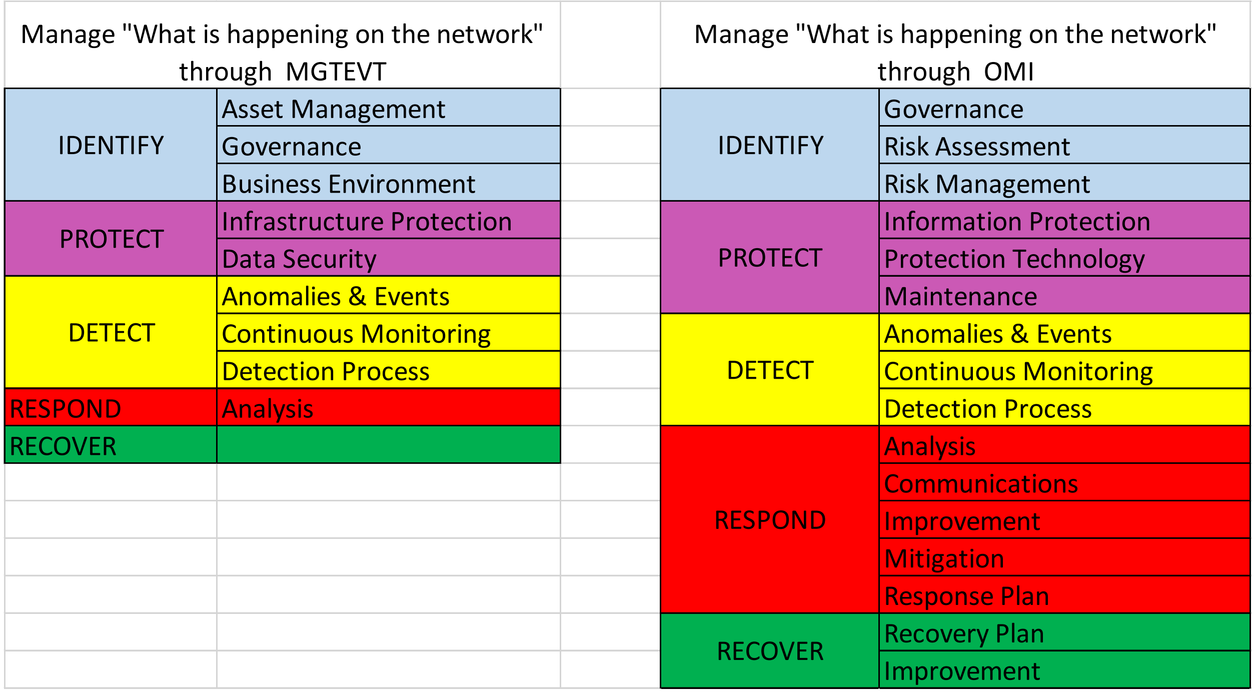
The set of tables in Figure 5 show the relationship of the Cybersecurity Framework categories to the CDM Phases.

Manage "What is on the Network?"	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Data Security
	Information Protection
	Maintenance
DETECT	Anomalies & Events
	Continuous Monitoring
RESPOND	
RECOVER	

Manage "Who is on the network?"	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Access Control
	Awareness & Training
	Data Security
DETECT	Anomalies & Events
	Continuous Monitoring
RESPOND	Communications
RECOVER	

Manage "What is happening on the network" through BOUND	
IDENTIFY	Asset Management
	Governance
	Risk Assessment
PROTECT	Access Control
	Data Security
	Infrastructure Protection
	Protection Technology
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	
RECOVER	

Manage "What is happening on the network" through DBS	
IDENTIFY	Business Environment
	Governance
	Risk Assessment
	Risk Management
PROTECT	Information Protection
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
RECOVER	



Manage "What is happening on the network" through MGTEVT	
IDENTIFY	Asset Management
	Governance
	Business Environment
PROTECT	Infrastructure Protection
	Data Security
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
RECOVER	

Manage "What is happening on the network" through OMI	
IDENTIFY	Governance
	Risk Assessment
	Risk Management
PROTECT	Information Protection
	Protection Technology
	Maintenance
DETECT	Anomalies & Events
	Continuous Monitoring
	Detection Process
RESPOND	Analysis
	Communications
	Improvement
	Mitigation
	Response Plan
RECOVER	Recovery Plan
	Improvement

Figure 5-CDM mapping to Cybersecurity Framework Core Functions and Categories

I - 3 CDM and NIST Risk Management Framework

The CDM desired state attribute values represent a security posture for an information system as delineated within NIST SP 800-37 (Risk Management Framework [RMF]). Two key representations of the RMF are of direct concern to CDM. The first is shown in the RMF Organization Tiers as shown in the Figure 6, and the second is the process steps for the RMF as shown in Figure 7.

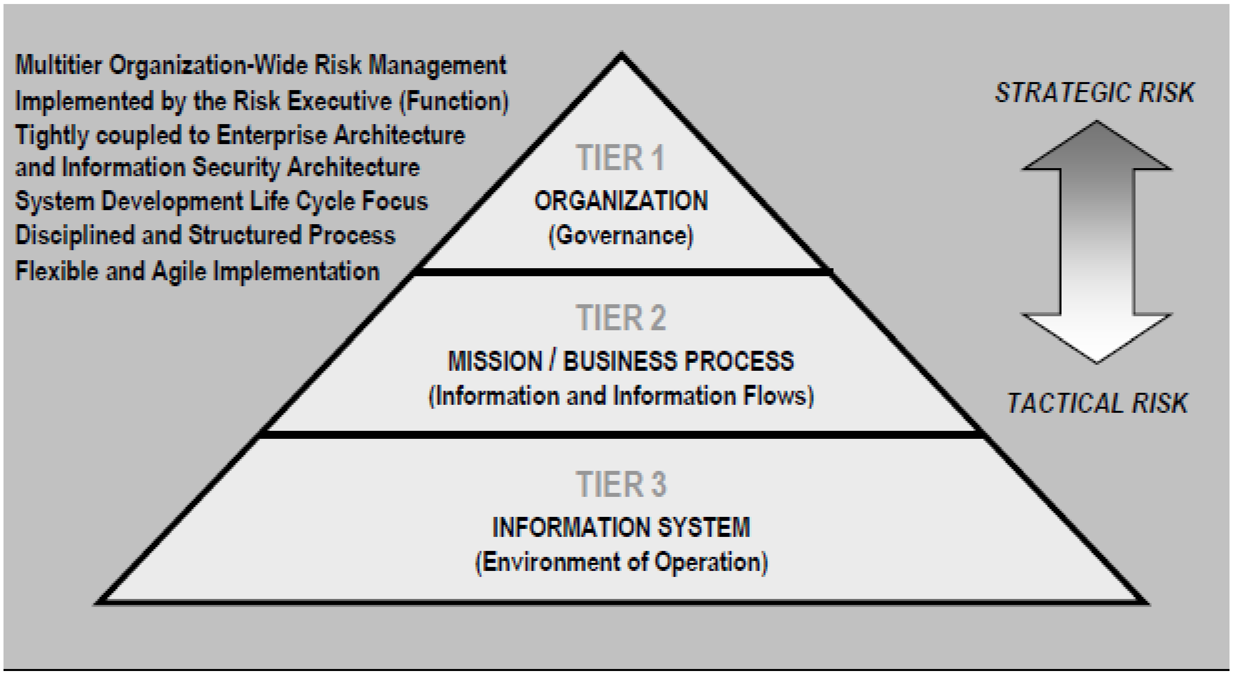

Multitier Organization-Wide Risk Management
Implemented by the Risk Executive (Function)
Tightly coupled to Enterprise Architecture
and Information Security Architecture
System Development Life Cycle Focus
Disciplined and Structured Process
Flexible and Agile Implementation
TIER 1
ORGANIZATION
(Governance)
TIER 2
MISSION / BUSINESS PROCESS
(Information and Information Flows)
TIER 3
INFORMATION SYSTEM
(Environment of Operation)
STRATEGIC RISK
TACTICAL RISK

Figure 6-RMF OU Tiers

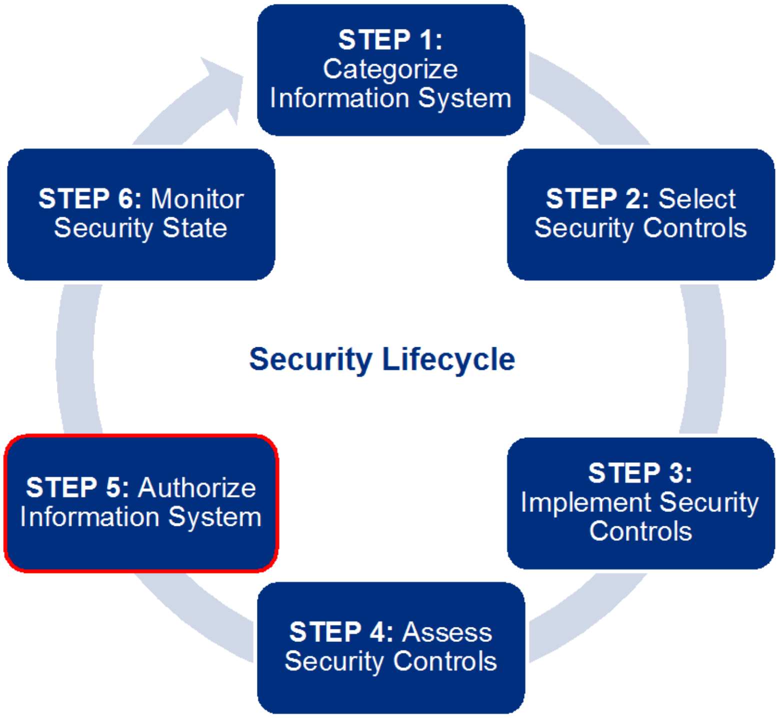

STEP 1: Categorize Information System
STEP 2: Select Security Controls
STEP 3: Implement Security Controls
STEP 4: Assess Security Controls
STEP 5: Authorize Information System
STEP 6: Monitor Security State
Security Lifecycle

Figure 7-RMF Process Steps (Cyclical)

Thus, CDM actual state data attributes can be associated with the implementation of NIST SP 800-53 controls[1] for an information system, specifically as referenced in the RMF process cycle. Additional attributes may be organizationally defined based on other security standards and guidelines, especially in support of the RMF Organization and Mission/Business Process Tiers.

Under this topic, there are three distinct areas of discussion:

1. Role of CDM with Ongoing Assessment
2. Role of CDM with Ongoing Authorization
3. The role of specific NIST SP 800-53 controls to CDM

The relationship of these CDM areas to the overall RMF Process Steps is shown in the following table:

RMF Step	Definition	CDM Defined Activity
1	CATEGORIZE Information System	Establish each Agency information system within its own FISMA container to include its relationship to assets and policies within the CDM Agency Dashboard.

[1] While this document uses NIST SP 800-53 controls to describe CDM desired states, controls are not limited to NIST SP 800-53 but include any security control (safeguard or countermeasure) that can support CDM desired state measurement of the security posture of an information system.

2	SELECT Security Controls	For each FISMA system based on FIPS 199 rating and Agency policies, tailor NIST SP 800-53 controls and align to operationalized CDM capabilities.
3	IMPLEMENT Security Controls	Utilize CDM-provided capabilities for those controls for which the assessment of their effectiveness can be automated.
4	ASSESS Security Controls	Performed on an ongoing basis by leveraging the CDM integration system ability to aggregate and correlate actual state data against desired state specific to each affected NIST SP 800-53 control.
5	AUTHORIZE Information System	Provides standardized measurements and visibility into deviations that might change risk assessment and authorization determinations.
6	MONITOR Security Controls	Provides authorizing officials and other parties of interest with automated and ongoing situational awareness of system status through risk scoring.

I - 3.1 Ongoing Assessment and CDM

Agencies are expected to perform information and information system risk assessments to support the authorization of systems to operate. Based on the risk assessment process for Agency information and information systems and to be consistent with the RMF step 2, appropriate NIST SP 800-53 controls must be implemented (RMF Step 3) to prevent system compromise and protect sensitive information.

Based on the activities of a threat actor, security events could immediately indicate a compromise and/or failure of one or more NIST SP 800-53 controls. In other cases, such as Advanced Persistent Threat and Zero Day threats, additional assessment and investigation may be needed to determine the underlying cause of the event and appropriate countermeasure response. These events may indicate a state change for the implementation of a NIST SP 800-53 control on a system. Continuously monitoring events for these state changes enables ongoing assessment of NIST SP 800-53 controls (RMF Step 4). State changes related to these security controls may or may not increase system risk, and need to be passed to the ongoing authorization risk management process to determine changes in the risk level of the system, which is the interaction of ongoing assessment with ongoing authorization.

I - 3.2 Ongoing Authorization and CDM

The output of ongoing assessment identifies events that represent state changes in the implementation of NIST SP 800-53 controls (RMF Step 5). Ongoing authorization identifies events that represent potential increases in security risks as incidents. The primary policy that is associated with the requirement for agencies to perform Ongoing Authorization (and by inference ongoing assessment) is OMB A-130, “Managing Information as a Strategic Resource,” and its associated guidance.

Incidents may indicate an unacceptable state change for the implementation of a NIST SP 800-53 control on a system. Based on state changes related to these security controls and the responses to incidents, CDM performs the Ongoing Authorization risk management process to determine changes in the security risk level of the system and whether the security risk level remains acceptable to support continued authorization and operation.

Failure to respond to mismatches between the desired and actual state, respond and recover from a security incident, or use shared information to protect the system from known threats increases risk to the system and organization and could result in suspension of the authorization to operate by the authorizing official.

I - 3.3 Leveraging NIST SP 800-53 Controls

The standard practice for the documentation of an information system’s security posture characteristics is used by following the process defined in NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, {Reference 10} which provides a significant amount of the practical context for working within the RMF as established in NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.*” {Reference 13} This is specifically identified as Step 6 in the RMF Process Cycle.

The full details for all CDM desired state policies, attributes, and examples for the following 17 NIST SP 800-53 control families will be available as government-furnished information from the CDM Program Management Office:

- Security Controls in the Access Control (AC) family address the ability to allow authorized subjects to gain access to system resources and data, and to prevent all other accesses. Most of the AC controls are linked to attributes of the FISMA Container to express desired state for system access. Organization-level controls (e.g., AC-1) are associated with the OU Container, while specific controls related to users and permissions are related to attributes in the MUR. AC controls used to derive the CDM desired states are: AC-1, AC-2 (1) (2) (3) (4) (5) (11) (12) (13), AC-3, AC-4, AC-5, AC-6 (1) (2) (3) (5) (9) (10), AC-7, AC-8, AC-10, AC-11 (1), AC-12, AC-14, AC-17 (1) (2) (3) (4), AC-18 (1) (4) (5), AC-19 (5), AC-20 (1) (2), AC-21, AC-22.

- Security Controls in the Awareness and Training (AT) family address that system designers, administrators, operators, and users have the appropriate training to securely perform their roles. The controls ensure that users understand cybersecurity threats and concerns, and that they are cognizant of the threats the organization faces and their responsibilities in defending against them. Most of the AT controls are linked to the attributes of the OU Container to express desired state for training. Organization-level controls (e.g., AT-1) are associated with the OU Container, while specific controls related to the implementation of training users are related to attributes in the MUR. AT controls used to derive the CDM desired states are: AT-1, AT-2 (2), AT-3, AT-4.

- Security Controls in the Audit and Accountability (AU) family address the ability to record actions that occur in the system, to analyze those records, and to correctly attribute each action to the entity that caused it to happen. Most of the AU controls are linked to attributes of the FISMA Container to express desired state for auditing. Organization-level controls (e.g., AU-1) are associated with the OU Container, while specific controls related to the implementation of auditing on system components are related to Configuration Settings Management (CSM) attributes in the MDR. AU controls used to derive the CDM desired states are: AU-1, AU-2 (3), AU-3 (1) (2), AU-4, AU-5 (1) (2), AU-6 (1) (3) (5) (6), AU-7 (1), AU-8 (1), AU-9 (2) (3) (4), AU-10, AU-11, AU-12 (1) (3).

- Security Controls in the Security Assessment and Authorization (CA) family address the steps involved in authorizing a system to operate under specific conditions in a specific environment with a defined and acceptable level of risk. Security Assessment is the process of determining what a system's characteristics and risk level are; Authorization is the process of granting (or denying) approval to operate under a defined set of conditions. Most of the CA controls are linked to attributes of the FISMA Container to express desired state for assessment and authorization. Organization-level controls (e.g., CA-1) are associated with the OU Container, while specific controls related to the personnel performing assessments and authorizations are related to attributes of the MUR. Controls addressing connections between systems are related to attributes in the MSR with a corresponding linkage to CSM attributes in the MDR. CA controls used to derive the CDM desired states are: CA-1, CA-2 (1) (2), CA-3 (5), CA-5, CA-6, CA-7 (1), CA-8, CA-9.
- Security Controls in the Configuration Management (CM) family address the steps involved in understanding and controlling the components of a system and how those components are configured. The goal is to ensure that all components of the system operate as expected, that there is no component that is unexamined or not understood, and that all changes have been carefully considered and their impacts are understood before they are made. Most of the CM controls are linked to attributes of the FISMA Container to express desired state for configuration management. Organization-level controls (e.g., CM-1) are associated with the OU Container, while specific controls related to the personnel performing configuration management functions are related to attributes of the MUR. The specific implementation of system configurations is related to CSM attributes of the MDR. CM controls used to derive the CDM desired states are: CM-1, CM-2 (1) (2) (3) (7), CM-3 (1) (2), CM-4 (1), CM-5 (1) (2) (3), CM-6 (1) (2), CM-7 (1) (2) (5), CM-8 (1) (2) (3) (4) (5), CM-9, CM-10, CM-11.
- Security Controls in the Contingency Planning (CP) family address whether the system can operate and carry out its mission despite any defined set of events that may occur. Those events may be natural disasters (e.g., hurricanes, floods), unintentional (e.g., a power failure) or intentional (e.g., an attack by an adversary). The controls ensure that the organization has considered events that may occur; believes that it understands how likely each event is and what its impact may be; and can respond should the event occur. Most of the CP controls are linked to attributes of the FISMA Container to express desired state for contingency planning. Organization-level controls (e.g., CP-1) are associated with the OU Container, while specific controls related to personnel performing contingency planning functions are related to attributes of the MUR. The specific implementation of controls related to backup operations on system components is related

to CSM attributes of the MDR. CP controls used to derive the CDM desired states are: CP-1, CP-2 (1) (2) (3) (4) (5) (8), CP-3 (1), CP-4 (1) (2), CP-6 (1) (2) (3), CP-7 (1) (2) (3) (4), CP-8 (1) (2) (3) (4), CP-9 (1) (2) (3) (5), CP-10 (2) (4).

- Security Controls in the Identification and Authentication (IA) family address knowing who or what each entity in the system is and on whose behalf it is operating. Identification means being able to associate a unique name with each entity—individual user, group of users, device, program, network component—in the system. Authentication means providing proof that the user of an identifier is authorized to use that identifier (e.g., that this user is the correct human user). Most of the IA controls are linked to attributes of the FISMA Container to express desired state for identification and authentication. Organization-level controls (e.g., IA-1) are associated with the OU Container, while specific controls related to personnel performing identification and authentication management are related to attributes of the MUR. The specific implementation of controls related to authentication of users is related to CSM attributes of the MDR. IA controls used to derive the CDM desired states are: IA-1, IA-2 (1) (2) (3) (4) (8) (9) (11) (12), IA-3, IA-4, IA-5 (1) (2) (3) (11), IA-6, IA-7, IA-8 (1) (2) (3) (4).
- Security Controls in the Incident Response (IR) family address how the organization will respond to a security incident that occurs during operation. Security incidents include attempted or successful attacks; failures of security-related system components; and suspected or actual misbehavior by system users. Most of the IR controls are linked to attributes of the FISMA Container to express desired state for incident response. Organization-level controls (e.g., IR-1) are associated with the OU Container, while specific controls related to personnel performing incident response functions are related to attributes of the MUR. Specific activities related to incident response actions are related to attributes of the MIR. IR controls used to derive the CDM desired states are: IR-1, IR-2 (1) (2), IR-3 (2), IR-4 (1) (4), IR-5 (1), IR-6 (1), IR-7 (1), IR-8.
- Security Controls in the Maintenance (MA) family address events that occur in ensuring that the system is operating correctly, is updated when needed, and can be repaired with minimal security impact when a problem does occur. Most of the MA controls are linked to attributes of the FISMA Container to express desired state for maintenance. Organization-level controls (e.g., MA-1) are associated with the OU Container, while specific controls related to personnel associated with maintenance processes are related to attributes of the MUR. MA controls used to derive the CDM desired states are: MA-1, MA-2 (2), MA-3 (1) (2) (3), MA-4 (2) (3), MA-5 (1), MA-6.
- Security Controls in the Media Protection (MP) family address the creation, management, distribution, storage, and disposal of electromagnetic or optical storage media. Media can include DVDs, CDs, USB drives, hard drives, etc. Security controls in this family cover physical and logical access to media; proper electronic and physical marking of media; and use, storage, transport, and disposal of media. Most of the MP controls are linked to attributes of the FISMA Container to express desired state for media protection. Organization-level controls (e.g., MP-1) are associated with the OU Container, while specific controls related to personnel associated with media protection processes are related to attributes of the MUR. The specific implementation of controls related to media protection on system components is related to CSM attributes of the MDR. MP controls

used to derive the CDM desired states are: MP-1, MP-2, MP-3, MP-4, MP-5 (4), MP-6 (1) (2) (3), MP-7 (1).

- Security Controls in the Physical and Environmental Protection (PE) family address controlling the spaces in which system components operate to ensure that components cannot be accessed, modified, replaced, stolen, or removed in a manner that would violate security policy.

  Security controls in this family also address system damage that could be caused by fire, water, electrical failure, or other related issue.

  Most of the PE controls are linked to attributes of the FISMA Container to express desired state for physical and environmental protection. Organization-level controls (e.g., PE-1) are associated with the OU Container, while specific controls related to personnel associated with physical and environmental protection processes are related to attributes of the MUR. Where the specific implementation of controls for physical access protections use a Physical Access Control System (PACS) on the network, those controls are related to CSM attributes of the MDR for the PACS. The specific implementation of environmental protection controls on system components is related to CSM attributes of the MDR. PE controls used to derive the CDM desired states are: PE-1, PE-2, PE-3 (1), PE-4, PE-5, PE-6 (1) (4), PE-8 (1), PE-9, PE-10, PE-11 (1), PE-12, PE-13 (1) (2) (3), PE-14, PE-15 (1), PE-16, PE-17, PE-18.

- Security Controls in the Planning (PL) family address the organization’s security plans. Factors include how the plan is developed; contents of the plan; and the plan’s impact on security, privacy, and organizational operations. Most of the PL controls are linked to attributes of the FISMA Container to express desired state for planning. Organization-level controls (e.g., PL-1) are associated with the OU Container, while specific controls related to information system users and personnel associated with planning processes are related to attributes of the MUR. PL controls used to derive the CDM desired states are: PL-1, PL-2 (3), PL-4 (1), PL-8.

- Security Controls in the Personnel Security (PS) family address vetting of the authorized organizational users of the system and system components. The goal is to ensure that all people with access to the system have earned the level of trust required of them to access the system and use information system data in a way that conforms to policy. Most of the PS controls are linked to attributes of the OU Container to express desired state for personnel security. Specific controls related to users and personnel associated with personnel security processes are related to attributes of the MUR. PS controls used to derive the CDM desired states are: PS-1, PS-2, PS-3, PS-4 (2), PS-5, PS-6, PS-7, PS-8.

- Security Controls in the Risk Assessment (RA) family address that the development, deployment, and operation of the system is controlled by and is compatible with the organization’s overall risk assessment process. That is, the risk incurred by developing, deploying, and operating the system is understood and accepted by the organization. The RA controls are split between links to attributes of the FISMA Container and the OU Container. Specific controls related to personnel associated with risk assessment processes are related to attributes of the MUR. RA controls used to derive the CDM desired states are: RA-1, RA-2, RA-3, RA-5 (1) (2) (4) (5).

- Security Controls in the System and Services Acquisition (SA) family address how the organization acquires and operates the system. The control family covers the entire system life cycle, from initial design to ultimate decommissioning. The controls ensure that proper security engineering principles and practices are used in all phases of the life cycle.

  This control family includes how the organization selects and uses contractors and partners where needed to provide/support an information system.

  Most of the SA controls are linked to attributes of the OU Container to express desired state for system and services acquisition and Supply Chain Risk Management (SCRM). Where the implementation of specific development and acquisition controls is defined for individual information systems, those controls are linked to the FISMA Container. Controls incorporating SCRM activities are related to attributes in the MDR. Specific controls related to personnel associated with system and services acquisition processes are related to attributes of the MUR. SA controls used to derive the CDM desired states are: SA-1, SA-2, SA-3, SA-4 (1) (2) (9) (10), SA-5, SA-8, SA-9 (2), SA-10, SA-11, SA-12, SA-15, SA-16, SA-17.

- Security Controls in the System and Communications Protection (SC) family address how the system is designed and operated to detect and defeat attempted attacks. Controls include architectural principles such as partitioning; the use and protection of boundaries; the use of cryptography (including Public Key Infrastructure); and providing defenses against denial-of-service attacks. Most of the SC controls are linked to attributes of the FISMA Container to express desired state for physical and environmental protection. Organization-level controls (e.g., SC-1) are associated with the OU Container. The specific implementation of controls related to external connections/communications is related to attributes of the MSR. The specific implementation of controls related to system and communications protections internal to the information system is related to CSM attributes of the MDR. SC controls used to derive the CDM desired states are: SC-1, SC-2, SC-3, SC-4, SC-5, SC-7 (3) (4) (5) (7) (8) (18) (21), SC-8 (1), SC-10, SC-12 (1), SC-13, SC-15, SC-17, SC-18, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-28, SC-39.

- Security Controls in the System and Information Integrity (SI) family address protecting the system from attacks using malicious code; monitoring system behavior to detect flaws or attacks; and acting to remediate the situation when a flaw or attack is detected. Most of the SI controls are linked to attributes of the FISMA Container to express desired state for system and information integrity. Organization-level controls (e.g., SI-1) are associated with the OU Container, while specific controls related to personnel associated with information system monitoring processes are related to attributes of the MUR. The specific implementation of controls related system and information integrity and monitoring is related to CSM attributes of the MDR. SI controls used to derive the CDM desired states are: SI-1, SI-2 (1) (2), SI-3 (1) (2), SI-4 (2) (4) (5), SI-5 (1), SI-6, SI-7 (1) (2) (5) (7) (14), SI-8 (1) (2), SI-10, SI-11, SI-12, SI-16.

I - 4 Defining CDM from Attachment N Requirement's Documents

Historically, the definition of what was CDM content was established through discussion of its capabilities. This section provides an overview of how the original Attachment N documents and corresponding tool functional areas (TFAs) for each CDM phase map to the Phased Detailed Requirements (Table *2*) as described below. The material following this table presents a synopsis of each of the Attachment N documents.

DHS CDM Phase Attachments	Phased Detailed Requirements	CDM/CMaaS Blanket Purchase Agreement (BPA) TFAs
Phase 1 Attachment N Requirements	Manage "What is on the network?"	• TFA 1 – Hardware Asset Management • TFA 2 – Software Asset Management • TFA 3 – Configuration Settings Management • TFA 4 – Vulnerability Management
Phase 2 Attachment N-2 Requirements	Manage "Who is on the network?"	• TFA 6 – Manage Trust in People Granted Access • TFA 7 – Manage Security-Related Behavior • TFA 8 – Manage Credential and Authentication • TFA 9 – Manage Account/Access/Manage Privileges
Phase 3 Attachment N-BOUND Requirements	Manage "How is the network protected?"	• TFA 5 – Manage Network Access Controls
Phase 3 Attachment N-3-Manage Events (MNGEVT) Requirements	Manage "What is happening on the network?" for MNGEVT	• TFA 10 – Prepare for Contingencies and Incidents • TFA 11 – Respond to Contingencies and Incidents • Ongoing Assessment
Phase 3 Attachment N-3-Design and Build in Security (DBS) Requirements	Manage "What is happening on the network?" for DBS	• TFA 12 – Design and Build in Requirements Policy and Planning • TFA 13 – Design and Build in Quality • Supply Chain Risk Management
Phase 3 Attachment N-3-Operate, Monitor, and Improve (OMI) Requirements	Manage "What is happening on the network?" for OMI	• TFA 14 – Manage Audit Information • TFA 15 – Manage Operation Security • Ongoing Authorization

Table 2: CDM Phased Attachment-N Requirements and Associated CDM BPA Capabilities

Phase 1 - Manage "What is on the network?"

This phase is based on Phase 1 Attachment-N requirements.

Manage hardware and software baseline system inventory is based on the CDM Hardware Asset Management (HWAM) and Software Asset Management (SWAM) capabilities, which require the collection of device hardware and software components to establish the Agency's information system infrastructure computing environment. These CDM HWAM and SWAM capabilities cover verification and validation for the existence of hardware infrastructure devices, and the accurate identification of approved software components.

Hardware and software configurations are based on CSM requirements to ensure that hardware and software (specifically the operating system and installed applications) assets are securely configured and hardened.

Vulnerability Management (VUL) requirements extend the focus of SWAM to achieve a level of confidence that software is free from vulnerabilities. This CDM capability covers verification and validation that hardware devices have the correct security configuration settings, and the system platform is hardened to reduce the platform attack surface.

Phase 2 – Manage “Who is on the network?”

Manage users/accounts is based on Phase 2 Attachment-N2 management and control of account/access/managed privileges (PRIV), trust in people granted access (TRUST), credentials and authentication (CRED), and security-related behavior (BEHAVE) requirements that require the management and control of users as an asset to ensure that the right individual has appropriate access to the right resource. This supports “Who is on the network?”

This CDM capability covers the verification and validation of appropriate user privileges, assigned credentials, trustworthiness, appropriate user security behavior training, and appropriately granted resource access rights to users.

Phase 3 – Manage “How is the network protected?”

Network defense and infrastructure abnormal behavior is based on Phase 3 Attachment N-BOUND to defend network boundaries and identify abnormal behavior (of networks and users) that may indicate that a security incident has occurred. This supports “How is the network protected?”

This CDM capability covers verification and validation of logical and physical network interfaces to reduce intrusive, malicious, and disruptive attacks; cryptographic mechanisms ensure confidentiality and integrity of data on the network; and methods to identify security incidents.

Phase 3 – Manage “What is happening on the network?” for MNGEVT

Integrity of process and resultant materials is based on the Phase 3 Attachment-N-3-MNGEVT and Attachment-N-3-OMI requirements to prepare for security incidents/events (through processes, policies, and procedures), gather appropriate audit/log data from appropriate sources, and identify security events/incidents (network and user abnormal behavior) through the analysis of audit/log data. This supports “What is happening on the network?”

In addition, ongoing assessment is the continuous process of comparing security-related container and object attributes between the actual state and the desired state. This comparison is performed by the CDM PDP. The discrepancy between actual state and desired state reflects the level of effectiveness of control implementations and the overall security posture of the system. The results of the ongoing assessment are used to evaluate the changes in risk posture associated with the discrepancy. Ideally, the ongoing assessment process is fully automated, with the desired state being encoded in the CDM PDP and the actual state being collected using CDM sensors. This supports ongoing assessment.

This CDM capability covers verification and validation of processes, policies, and procedures supporting cybersecurity preparation, audit and log data collection, security analysis of audit/log data, and incident reporting to provide forensic evidence of malicious or suspicious behavior.

Phase 3 – Manage "What is happening on the network?" for DBS

Software assurance based on Phase 3 Attachment-N-3-DBS requirements ensures the level of confidence that the software is free from defects, either intentionally designed into the software or accidentally inserted at any time during its life cycle, and that the software functions in the intended manner. This supports the software element of "What is happening on the network?"

The U.S. government and critical infrastructure sectors are increasingly dependent on commercial products and systems, which present significant benefits including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. However, with some of these benefits there is an increase in the risk of a threat event that can directly or indirectly affect the supply chain, which often goes undetected and may result in risks to the acquirer. Therefore, SCRM seeks to enable the provisioning of the least vulnerable solutions to agencies through a robust assessment of supply chain risks, communication about those risks to the agencies, and appropriate response and monitoring of those risks throughout the entire system life cycle.

This CDM capability covers verification and validation of preventing and detecting software vulnerabilities to measure software assurance for built and acquired software components.

Phase 3 – Manage "What is happening on the network?" for OMI

Responding to and recovering from cyber incidents is based on Phase 3 Attachment-N-3-OMI requirements for incident prioritization and response, and post-incident activities (e.g., information sharing). This supports "What is happening on the network?"

Ongoing Authorization is the continuous evaluation of the change in risk level related to changes in security policies concerning object attributes (i.e., actual state and desired state) for threat behaviors that impact the security posture. This impact to security is measured by capturing changes in existing security safeguards (e.g., NIST SP 800-53 controls and countermeasures) and identifying new component weaknesses and vulnerabilities.

MNGEVT supports the runtime collection of attributes (actual state) and continuous monitoring of the policies related to attributes for ongoing assessment (actual state vs. desired state) to enhance current or apply new security controls and countermeasures. The results of the ongoing assessment will be used as inputs to the OMI Ongoing Authorization risk assessment process to determine if the level of risk remains acceptable for a given information system to support continued authorization and operation.

This CDM capability covers verification and validation of processes/procedures to prioritize incidents and associated response actions, quickly mitigate the impact of an incident, take appropriate remediation actions to eliminate the impact (restore normal operations) of the incident, and support information sharing and collaboration (both internal and external) to minimize or prevent the impact of future incidents.

I - 5 Conclusion

This document defines the multiple frameworks that have been applied to CDM solutions and establishes the different points of view that need to be represented in any discussion of the definition of the "best" security posture for "desired state."

The details of the requirements that are part of the CDM solution definition are provided in the companion volume (Volume Two), "CDM Technical Capabilities – Requirements Catalog."

References

1. Continuous Diagnostics and Mitigation (CDM) System Architecture: Architecture Principles Document, Version 0.5, August 31, 2016
2. Framework for Improving Critical Infrastructure Cybersecurity, Version 1.0, February 12, 2014
3. Phase 1: Attachment N Requirements, Section 9
4. Phase 2: Attachment N-2 Requirements, February 12, 2015
5. Phase 3: Attachment N-3-BOUND Requirements, 2nd Issue November 15, 2016
6. Phase 3: Attachment N-3-Manage Events Requirements, June 7, 2016
7. Phase 3: Attachment N-3-Operate, Monitor and Improve, August 5, 2016
8. Phase 3: Attachment N-3-Design and Build in Security, September 16, 2016
9. Framework for Improving Critical Infrastructure Cybersecurity Version 1.1 (draft), January 10, 2017
10. NIST SP 800-53, https://nvd.nist.gov/800-53/Rev4/
11. Security Requirements for Cryptographic Modules, FIPS 140-2, May 25, 2001, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.140-2.pdf
12. Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, February 2004, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
13. NIST SP 800-37R1, 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
14. Common Platform Enumeration (CPE) https://nvd.nist.gov/products/cpe
15. Common Configuration Enumeration (CCE) https://nvd.nist.gov/config/cce/index
16. Common Vulnerability Enumeration (CVE) https://nvd.nist.gov/vuln/search
17. NISTIR 7502 The Common Configuration Scoring System (CCSS): Metrics for Software Security Configuration Vulnerabilities, December 2010, http://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7502.pdf
18. National Vulnerability Database (NVD) https://nvd.nist.gov/
19. Common Vulnerability Scoring System CVSS https://nvd.nist.gov/vuln-metrics/cvss
20. Federated Identity, Credential, and Access Management (FICAM) https://www.idmanagement.gov/IDM/s/article_content_old?tag=a0Gt0000000XNYG
21. Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks (X.509 ITU-T) http://www.itu.int/rec/T-REC-X.509/en
22. Personal Identity Verification (PIV) of Federal Employees and Contractors, FIPS 201-2, August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
23. Common Weakness Enumeration (CWE) https://nvd.nist.gov/vuln/categories
24. US-CERT Federal Incident Notification Guidelines
25. HPE Security ArcSight Common Event Format, version 23, May 16, 2016
26. Guide to the Software Engineering Body of Knowledge, version 3.0, 2014

27. Security Content Automation Protocol (SCAP) https://scap.nist.gov/

III - Appendix A: Acronyms, Terms and Definitions

Acronym	Term	Definition
	Attributes	A set of labels, values, and hierarchies that describe a characteristic or dimension of a CDM object.
	Attribute Values	A list of possible value assignments or types for an attribute.
	BOUND	BOUND provides boundary protection for the interior of the network from all interconnections to other external networks.
	Data Element	A piece of information about CDM objects, their attributes, and/or associated policy to support the identification of defects.
	CDM Dashboard	The tool that aggregates and displays CDM information at the Agency or Federal level. The dashboard provides consistent, timely, targeted, and prioritized information to security decision makers from cross-agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first.
AC	Access Control	This family of controls addresses the ability to allow authorized subjects to gain access to system resources and data, and to prevent all other accesses.
AT	Awareness and Training	This family of controls addresses that system designers, administrators, operators, and users have the appropriate awareness and training to securely perform their roles.
AU	Audit and Accountability	This family of controls addresses the ability to record actions that occur in the system, to analyze those records, and to correctly attribute each action to the entity that caused it to happen.
BEHAVE	Manage Security-Related Behavior	The BEHAVE capability ensures that authorized users with or without special security responsibilities exhibit the appropriate behavior for their role.

Acronym	Term	Definition
CA	Security Assessment and Authorization	This family of controls addresses the steps involved in authorizing a system to operate under specific conditions in a specific environment with a defined and acceptable level of risk.
CDM	Continuous Diagnostics and Mitigation	Provides Federal Departments and Agencies with capabilities and tools that identify cybersecurity risks on an ongoing basis, prioritize these risks based upon potential impacts, and enable cybersecurity personnel to mitigate the most significant problems first. Congress established the CDM program to provide adequate, risk-based, and cost-effective cybersecurity and allocate cybersecurity resources more efficiently.
CM	Configuration Management	This family of controls addresses the steps involved in understanding and controlling the components of a system and how those components are configured.
CMaaS	Continuous Monitoring as a Service	The collection of elements that are not in the scope of the Dashboard.
CP	Contingency Planning	This family of controls addresses whether the system can operate and carry out its mission despite any defined set of events that may occur.
CRED	Credentials and Authentication Management	The CRED capability ensures that only proper credentials are authenticated to systems, services, and facilities.
CSF	Cybersecurity Framework	OMB Memorandum 16-03, “Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements,” calls out the federal adoption of the NIST Cybersecurity Framework (CSF) for improving critical infrastructure cybersecurity.
CSM	Configuration Settings Management	CSM ensures that authorized security configuration benchmarks exist and contain acceptable value(s) for each relevant configurable setting for each IT asset type.
CVE	Common Vulnerability Enumeration	A dictionary of common names (i.e., CVE Identifiers) for publicly known cybersecurity vulnerabilities.

Acronym	Term	Definition
CVSS	Common Vulnerability Scoring System	CVSS provides an open framework for communicating the characteristics and impacts of IT vulnerabilities.
CWE	Common Weakness Enumeration	The CWE Specification provides a common language for discussing, finding, and dealing with the causes of software security vulnerabilities found in code, design, or system architecture.
DBS	Design and Build in Security	Describes preventing exploitable vulnerabilities from being effective in the software/system while in development or deployment.
DHS	Department of Homeland Security	Federal Agency whose missions include preventing terrorism and enhancing security; managing our borders; administering immigration laws; securing cyberspace; and ensuring disaster resilience.
FISMA	Federal Information Security Modernization Act 2014	The U.S. legislation that defines a comprehensive framework to protect Government information, operations and assets against natural or man-made threats. FISMA was signed into law part of the Electronic Government Act of 2002. [2014 Act changed Management to Modernization.]
HWAM	Hardware Asset Management	The HWAM Function is to discover unauthorized or unmanaged hardware on a network.
IA	Identification and Authentication	This family of controls addresses knowing who or what each entity in the system is and on whose behalf, it is operating.
IR	Incident Response	This family of controls addresses how the organization will respond to a security incident that occurs during operation.
IT	Information Technology	Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

Acronym	Term	Definition
MA	Maintenance	This family of controls addresses events that occur in ensuring that the system is operating correctly, is updated when needed, and can be repaired with minimal security impact when a problem does occur.
MDR	Mater Device Record	A set of attributes or assertions about a user, with the device as the primary key.
MIR	Master Incident Record	Represents activities associated with security controls that require an action when an event occurs; deals with “what is happening on the network?”
MNGEVT	Manage Events	Describes preparing for events/incidents, gathering appropriate data from appropriate sources, and identifying incidents through analysis of data.
MP	Media Protection	This family of controls addresses the creation, management, distribution, storage, and disposal of electromagnetic or optical storage media.
MSR	Master System Record	A set of attributes or assertions about a user, with the system as the primary key.
MUR	Master User Record	A set of attributes or assertions about a user, with the user as the primary key.
NIST	National Institute of Standards and Technology	The Federal technology Agency that works with industry to develop and apply technology, measurements, and standards.
OMB	Office of Management and Budget	OMB is the business division of the Executive Office of the President of the United States that administers the United States federal budget and oversees the performance of federal agencies.
OMI	Operate, Monitor and Improve	Describes audit data collection and analysis, incident prioritization and response, and post-incident activities (e.g., information sharing).
OU	Organizational Unit	The Government Department or Agency responsible for the information system.

Acronym	Term	Definition
PACS	Physical Access Control System	An automated system that manages the passage of people or assets through an opening(s) in a secure perimeter(s) based on a set of authorization rules.
PDP	Policy Decision Point	Repository for policies that are distributed to enforcement points; mediates or de-conflicts DPs per MPs in some implementations.
PE	Physical and Environmental Protection	This family of controls addresses the controlling of the spaces in which system components operate, to ensure that components cannot be accessed, modified, replaced, stolen, or removed in a manner that would violate security policy.
PEP	Policy Enforcement Point	A service that resides on and directly interacts with network objects (e.g., servers, asset scanners, firewalls), which exchanges policy-related messages with the Policy Decision Point. The PEP enforces organizational policy via the configuration applied to the object.
PL	Planning	This family of controls addresses the organization’s security plans. Factors include how the plan is developed; contents of the plan; and the plan’s impact on security, privacy, and organizational operations.
PRIV	Managing Account Access Capability	This CDM capability is to provide an agency the assurance that users and systems have access to, and control of, only the appropriate resources. The capability identifies access beyond what is needed to meet business requirements.
PS	Personnel Security	This family of controls addresses vetting of the authorized organizational users of the system and system components.
RA	Risk Assessment	This family of controls addresses that the development, deployment, and operation of the system is controlled by and is compatible with the organization’s overall risk assessment process.
RMF	Risk Management Framework	A structured approach used to oversee and manage risk for an enterprise.
SA	System and Services Acquisition	This family of controls addresses how the organization acquires and operates the system.

Acronym	Term	Definition
SC	System and Communications Protection	This family of controls addresses how the system is designed and operated to detect and defeat attempted attacks.
SCRM	Supply Chain Risk Management	The process of identifying, assessing, and mitigating the risks associated with the distributed and interconnected nature of IT/operational technology (OT) product and service supply chains. It covers the entire life cycle of a system (including design, development, distribution, deployment, acquisition, maintenance, and destruction), as supply chain threats and vulnerabilities may intentionally or unintentionally compromise an IT/OT product or service at any stage.
SDLC	System Development Life Cycle	The process of planning, creating, testing, and deploying an information system. The SDLC concept applies to a range of hardware and software configurations, as a system can be composed of hardware only, software only, or a combination of both.
SI	System and Information Integrity	This family of controls addresses protecting the system from attacks using malicious code; monitoring system behavior to detect flaws or attacks; and acting to remediate the situation when a flaw or attack is detected.
SP	Special Publication	NIST Special Publications that include SP 800 subseries (computer security), SP 1800 subseries (NIST Cybersecurity Practice Guides) and selected SP 500-series (information technology) publications directly relevant to computer/cyber/information security and privacy
SWAM	Software Asset Management	The SWAM Function is to discover unauthorized or unmanaged software on a network.
TFA	Tool Functional Area	DHS is implementing the CDM program, made up of 15 BPA TFAs, that addresses “what is on the network,” “who is on the network,” and “what is happening on the network.”
TRUST	Manage Trust in People Granted Access Capability	This CDM capability assesses the inherent risk to an Agency from insider attacks for the purposes of granting trust to users and authorizing each user for certain attributes.

Acronym	Term	Definition
USB	Universal Serial Bus	An industry standard for connecting devices to computers.
VUL	Vulnerability Management	The VUL Function is to discover and support remediation of vulnerabilities in IT assets on a network as defined in NIST SP 800-53 controls.

Table 3: Acronyms, Terms and Definitions

III - Appendix B: Cybersecurity Framework Categories

Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.

Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.

Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.

Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.

Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.

Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, or devices, and to authorized activities and transactions.

Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are adequately trained to perform their information security-related duties and responsibilities consistent with related policies, procedures, and agreements.

Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.

Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.

Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components is performed consistent with policies and procedures.

Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.

Anomalies and Events (DE.AE): Anomalous activity is detected in a timely manner and the potential impact of events is understood.

Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.

Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure timely and adequate awareness of anomalous events.

Response Planning (RS.RP): Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.

Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.

Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.

Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and eradicate the incident.

Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.

Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure timely restoration of systems or assets affected by cybersecurity events.

Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.

Communications (RC.CO): Restoration activities are coordinated with internal and external parties, such as coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors.