cloudtamer.io

Fast Track Your Cloud Security

CDM Program Offers Unique Opportunity to Strengthen Cloud Infrastructure

What is CDM?

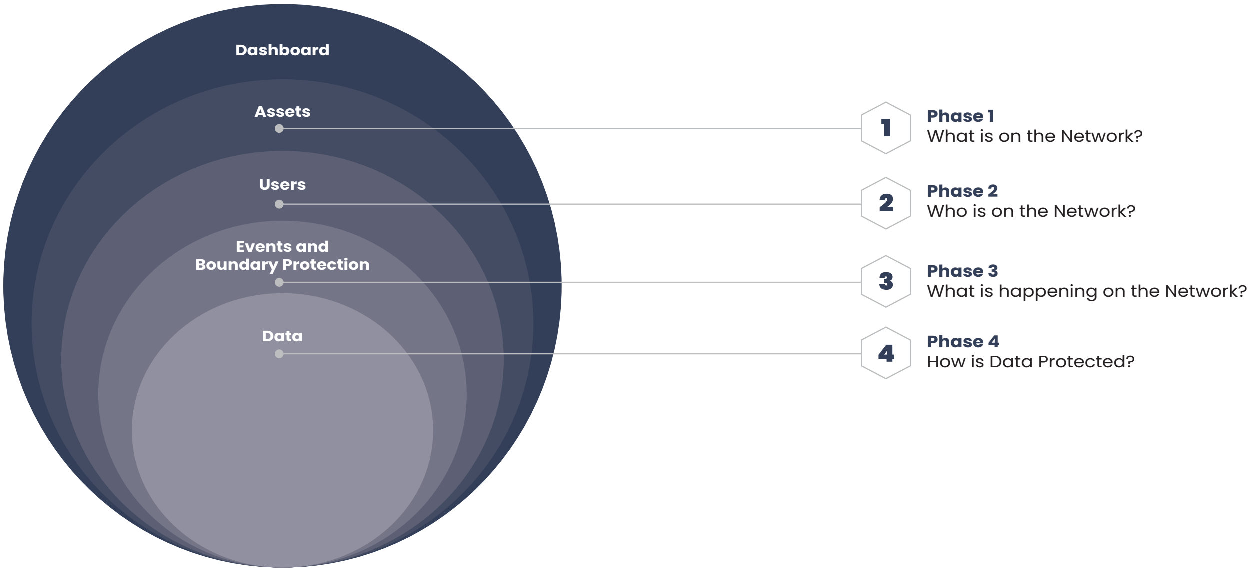
The Continuous Diagnostics and Mitigation (CDM) program is a United States government cybersecurity initiative led by the Department of Homeland Security (DHS) and the Cybersecurity and Infrastructure Security Agency (CISA). CDM aims to:

- Reduce agency threat surface
- Increase visibility into the federal cybersecurity posture
- Improve federal cybersecurity response capabilities
- Streamline Federal Information Security Modernization Act (FISMA) reporting

The Four Phases of CDM

To help agencies improve their cybersecurity posture, CISA defined four phases for agencies and private organizations to use as a model for their cybersecurity strategy.

When it comes to security in the cloud, there's room for increased focus. Agencies are expanding cloud procurements, but there is still significant confusion over governance and risk management of cloud infrastructure. Agencies may have solutions in place for operating system or database protection, but miss key requirements around protecting overall infrastructure.



Source: https://www.cisa.gov/cdm

When it comes to the cloud, these are the questions agencies must address across the four phases of CDM.

Phase	Cloud Infrastructure Questions
What is on the Network?	• What cloud resources exist across all your cloud service provider environments? • Who owns these resources and who is accountable for them? • Are they set up and configured securely and in compliance with your organization's policies?
Who is on the Network?	• Which users have access to your cloud resources? • Have these users been extended least privileges?
What is happening on the Network?	• How is data flowing through your cloud environments? • Are interactions being monitored on a continual basis?
How is Data Protected?	• What mechanisms have been put in place to ensure data is secure and cloud resources are continuously monitored to prevent security vulnerabilities?

How cloudtamer.io Helps with CDM for Cloud Security

From the moment cloud resources are provisioned until these resources are retired, a strong security posture is vital. From storage buckets and virtual instances to background services and logging, all cloud resources must be monitored and governed in a scalable, repeatable, and reportable way.

In addition to the management of an extensive array of services, users and user access must be carefully created and monitored. Personnel with a variety of skillsets – and levels of access - can make it difficult to keep track of who has permission to do what. Working across multiple cloud providers only compounds issues.

Through a single pane of glass, cloudtamer.io can automate account creation, apply and enforce policy, manage access control, provide financial reporting and actionable budget enforcements, and scan for continuous compliance across your cloud infrastructure. With out-of-the box policies and scans for NIST 800-53 Low/Moderate/High, NIST 800-171, CMMC L3, and CIS 1.2, agencies use cloudtamer.io to quickly achieve a strong security and compliance posture across multiple clouds.

cloudtamer.io is a DHS-approved product that provides the core functionality needed to achieve the CDM cloud infrastructure security requirements across all phases. Using cloudtamer.io, agencies have a complete 360-degree solution to prevent, detect, report, and remediate across their cloud infrastructure.

PHASE 1

Asset Management

How cloudtamer.io helps answer the question What is on the network?

In addition to understanding what hardware and software exists on the network, it's critical for agencies to understand their cloud account landscape to implement proper controls around access. cloudtamer.io enables your team to:

- Map cloud accounts and cloud resources across cloud service providers
- Implement continuous configuration monitoring against agency policies
- Assess vulnerability across cloud resources

PHASE 2

Identity and Access Management

How cloudtamer.io helps answer the question Who is on the network?

Ensuring least privileged access to cloud infrastructure and resources is a critical next step for agencies to undertake to minimize their threat surface. Access in the cloud can be complex, involving user and group memberships and nested relationships. cloudtamer.io enables your team to:

- Centrally visualize cloud users and access across all cloud accounts
- Streamline cloud account provisioning while ensuring least privilege permissions
- Manage policies to limit access to cloud resources and asset configurations
- Leverage a centralized identity management system to grant cloud access across cloud service providers

PHASE 3

Network Security Management

How cloudtamer.io helps answer the question What is happening on the network?

For agencies to respond to threats, you must understand what is happening on your cloud VPNs. This requires a mixture of both proactive boundaries and ongoing monitoring. cloudtamer.io enables your team to:

- Monitor network resources through scheduled and event-driven models
- Protect, monitor, and remediate network changes and configurations
- Provide continuous attestation that cloud accounts and resources meet desired requirements

PHASE 4

Data Protection Management

How cloudtamer.io helps answer the question How is data protected?

Visibility, proactive control via boundaries, and remediation: all of these are critical components to complete data protection. cloudtamer.io Cloud Rules establish these boundaries, ensuring only the right people have access to sensitive data. And cloudtamer.io compliance checks monitor and remediate security findings. cloudtamer.io enables your team to:

- Ensure data protection policies are enforced and are continually monitored
- Ensure cloud resource encryption is enforced through policy and boundaries
- Mitigate data loss impact by auto-remediation of security vulnerabilities
- Deploy incident response maneuvers in response to security findings

Use cloudtamer.io to succeed with CDM

cloudtamer.io is a DHS-approved solution designed to help government agencies meet their CDM requirements for securing and continuously monitoring their cloud resources.

Ready to get started? Contact our team to start taking advantage of the CDM program – with a bit of help from cloudtamer.io.

REQUEST A DEMO