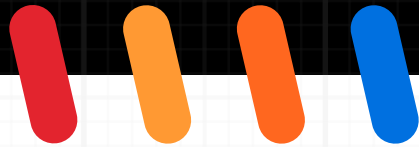


4 Keys to Better CDM Program Management

Build a more effective CDM management program,
hundreds of assets at a time



When the Department of Homeland Security launched the Continuous Diagnostics and Mitigation program a little over a decade ago, it represented a major shift in how federal agencies managed cyber risks on their networks.

Instead of doing it alone, DHS would provide agencies with tools so organizations could “continuously” monitor their networks for assets and risks.

Source: [Federal News Network](#)

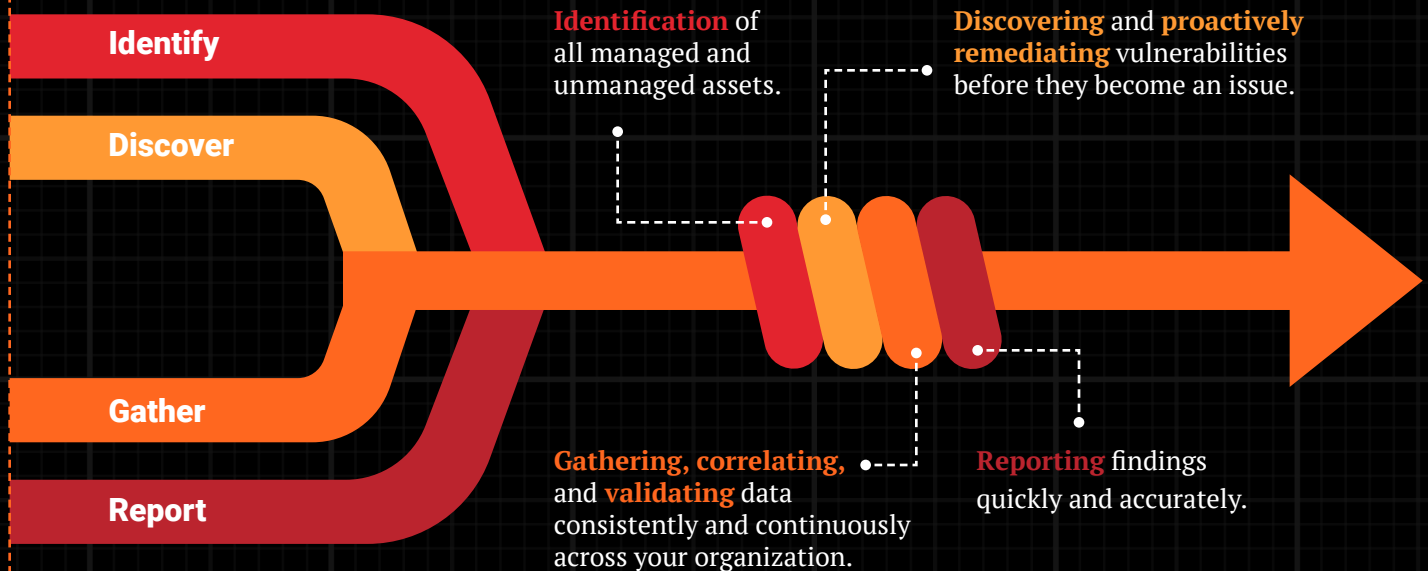
The Cybersecurity and Infrastructure Agency’s (CISA) Continuous Diagnostics and Mitigation (CDM) Program is one of the most mature and comprehensive cybersecurity programs ever introduced and is highly effective at mitigating cyber threats. But as agencies continue to add more assets and data, implementing it properly has become increasingly challenging.

It’s not unusual for a single organization to have multiple teams working with hundreds of disparate assets and data sets operating in separate silos. Some assets may be known to agency security managers, while others may be hidden in the shadows. And since data exists in multiple places, it can be difficult to trust that the information being reported to the CDM Dashboard is complete and accurate.

Fortunately, it’s possible to build an efficient and effective CDM compliance program. It starts with adopting a comprehensive approach to asset management, including asset identification, data and vulnerability management, and more.

Effective CDM management goes beyond asset tracking

An effective CDM program requires:



But identifying every asset and collecting and analyzing every data point is just scratching the surface. CDM Program compliance should also include:

- **Confirming assets are functioning properly** – and identifying the root cause if they aren't.
- **Tracking any changes or additions to assets** – to ensure that those changes do not cause security vulnerabilities.
- **Quickly responding to inquiries** – so that if CISA asks for an asset inventory report, you can quickly and accurately provide what is required.

Let's explore four tactics that correlate directly to each CDM Program objective, so you can increase visibility into your cybersecurity posture, reduce the threat surface, improve cybersecurity response capabilities, and streamline Federal Information Security Modernization Act (FISMA) reporting requirements.

CDM objective: Increase visibility into cybersecurity posture

Recommended tactic: Identify all assets across your organization

To fully protect your organization, you must identify, track, and manage every asset that uses your network, including both hardware and software assets. After all, you cannot secure what you can't see, or what you don't know exists.

75% of employees will acquire, modify, or create technology outside IT's visibility by 2027.

Source: [Gartner](#)

Yet manual asset tracking is extremely time consuming and resource intensive, especially considering that the average organization uses more than 200 applications¹ and an untold number of devices. Many assets exist in their own siloes, and many more might be invisible to IT administrators, thanks to users bringing their own devices and downloading unsanctioned applications.

What's more, the traditional method of tabulating assets in spreadsheets isn't only inefficient—it can lead to even greater security risks. Information could be incomplete, especially if teams are relying on data from others across the organization. This can result in hidden cybersecurity gaps that could compromise your agency's ability to successfully mitigate risk.

¹ Source: [The State of SaaS Sprawl in 2021](#), Productiv

86 hours – the amount of time it takes to perform a single manual asset audit.

Source: [Axonius](#)

To effectively satisfy CISA's call for comprehensive asset management and gain better visibility into your environment, you must automate your asset discovery processes. Automation allows you to:

To effectively satisfy CISA's call for comprehensive asset management and gain better visibility into your environment, you must automate your asset discovery processes. Automation allows you to:

- **Take stock of current assets** to reveal devices and applications that are already on the network, providing you with a complete view of all assets at a given moment.
- **Continuously detect** when new assets are added to the network.

The ability to perform asset discovery on-demand is also critical. When a known vulnerability like Sunburst, ProxyShell, or others begins to create havoc, being able to perform inventory as needed is critical. This enables the identification of affected assets, so potential issues can be proactively addressed.

Whether performing automated or on-demand discovery, the discovery process should be done in a way that is non-disruptive to the network. You cannot afford to add another process that uses up network resources and bandwidth. A discreet and behind the scenes inventory is essential so as to not to disrupt workflows—or your agency's mission.

Learn more about asset management.
Read our CDM Program blog series, beginning with
[The Foundations of DHS CDM: Hardware Asset Management](#)

CDM objectives: Increase visibility, reduce threat surface

Recommended tactic: Gather and correlate data to and from all sources

Ensuring the quality of your agency's data is essential to the success of the CDM program. Without accurate and high quality data, you will get inaccurate and low quality results that could compromise your ability to mitigate risk.

Many agencies use Configuration Management Databases (CMDBs) and monitor the quality of the data contained within them. The problem is that CMDBs are often only populated by one or two discovery sources. That does not do much good if you have hundreds of sources in your inventory. Relying solely on what a CMDB is showing can result in significant visibility gaps that could compromise your ability to ensure the data you're using is complete and accurate.

A comprehensive discovery process requires insights from all data sources, not just a limited number requiring manual intervention. This may include both known and previously unknown applications, managed and unmanaged mobile devices, and other ephemeral devices (devices that only last for a short period of time, like a virtual machine or container). Every possible asset producing or receiving data must be accounted for.

95%: increase in cyber attacks targeting government organizations worldwide in 2022.

Source: [Cloudsek](#)

Once the data is identified and collected it must be correlated with assets and combined and reconciled with the CMDB to form a complete view of your agency's security posture. By correlating collected data with assets, you can rapidly discover devices that might be missing critical patches or endpoint or configuration agents.

In short, you can use data from across your agency to effectively discover and close security gaps you may not have otherwise known existed. You'll practice both good asset and data protection management, checking off two important line items of the CDM Program.

Learn more about data correlation and its use in asset inventory. Read [Asset Inventory: The Correlation Problem](#)

CDM objectives: Reduce threat surface, improve response capabilities

Recommended tactic: Validate assets' adherence to security policies

Ensuring assets are in accordance with security policies is a core tenet of risk mitigation and compliance. In fact, CISA cites the ability to better comply with organizational security policies as one of the main benefits of asset management under the CDM Program.

Ensuring assets adhere to organizational security policies involves:

- **Continuous controls monitoring** – assets that stop adhering to security policies are automatically identified.
- **Security policy enforcement** – assets that do not adhere to security policies are automatically flagged and corrected.

If done incorrectly continuous monitoring can lead to alert overload that can impede your team's ability to effectively respond to high priority items. That's why automated policy enforcement is so important. Your system should have the ability to check assets against established security policies and automatically trigger corrective actions for devices, cloud assets, and users that are not complying with those policies. Corrective actions can include:

- **Isolating** devices from your network
- **Updating** vulnerability scans
- **Blacklisting** devices and applications
- **Disabling** users

Automated monitoring and remediation is key to maintaining a minimal threat surface while allowing IT teams to stay productive. They'll be able to focus on value-added tasks that advance your agency's mission while your security posture remains strong.

Learn more about [automated policy enforcement](#) and [how it works](#).

CDM objective: Streamline FISMA reporting

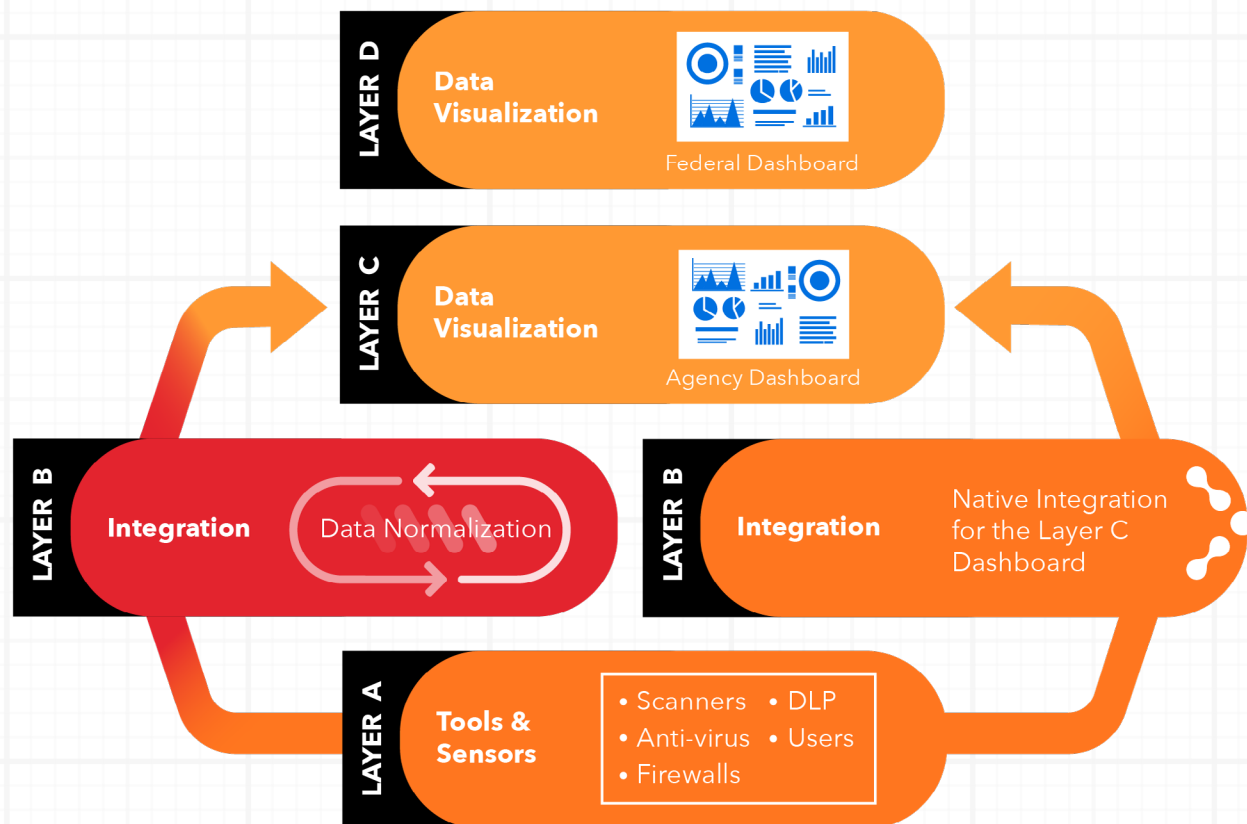
Recommended tactic: Tag assets and automate data transformation and reporting

55%: Percentage of federal agencies automatically reporting into the CDM dashboard (as of July 2023).

Source: Department of Homeland Security, [Strengthen Federal Cybersecurity](#)

More agencies are striking a good balance between delivering accurate reports on a regular basis and becoming more efficient. To continue that momentum, you need to be able to normalize the data you export to the CDM Dashboard while ensuring its accuracy.

This is done through the CDM data integration process. In this process, Defend Group Integrators collect data and create custom API tools (“CATS”) which connect to your agency’s assets. Integrators then transform the data to match data sets to the CDM Data Model, and results are exported into the CDM Dashboard.



But this is a complex process that takes a lot of time and resources to ensure it is done correctly and accurately. Automating the process removes much of that complexity and improves the accuracy of the reporting.

That starts with automating the correlation of data and assets (as described in the second tactic) and continues with asset tagging. This involves proactively tagging a single asset or groups of assets that must be routinely reported to ensure FISMA/CDM compliance. Tagging allows you to quickly generate reports on specific assets.

Reports can be exported to the CDM Dashboard or furnished on-demand; for example, in the event that CISA requests a report from a specific past date range. On-demand queries can instantly reveal vulnerabilities and coverage gaps and let you know the extent of the potential “blast radius” within your organization. You can quickly begin the remediation process, going beyond simple CDM reporting and into proactive vulnerability management and prevention.

Learn more about the role of data analytics in reporting. Read [How Data Analytics Reveals Asset Insights and Simplifies Reporting](#).

Enhance CDM Program management with Axonius Federal

The security tools you have are great collectors of information, but they operate in silos. You need to be able to aggregate data across tools to get a complete picture of your entire asset inventory and adhere to CDM Program requirements.

We augment and enhance your existing environments—and strengthen your security posture—by revealing what you have and identifying worrisome gaps. Hundreds of adapters allow you to see and control every asset in your agency. Our cybersecurity asset management and SaaS management solutions automatically and comprehensively identify assets, misconfigurations, and data security risks. We provide policy enforcement, accurate reporting, and more.

All of it makes Axonius the ultimate tool in your CDM Program management toolbox.

Learn how Axonius Federal Systems can help you improve CDM Program compliance.

Tour our platform or **reach out for a demo!**

axonius.com/axonius-federal
info@axoniusfed.com

**11130 Sunrise Valley Drive, STE 320
Reston, VA 20191**