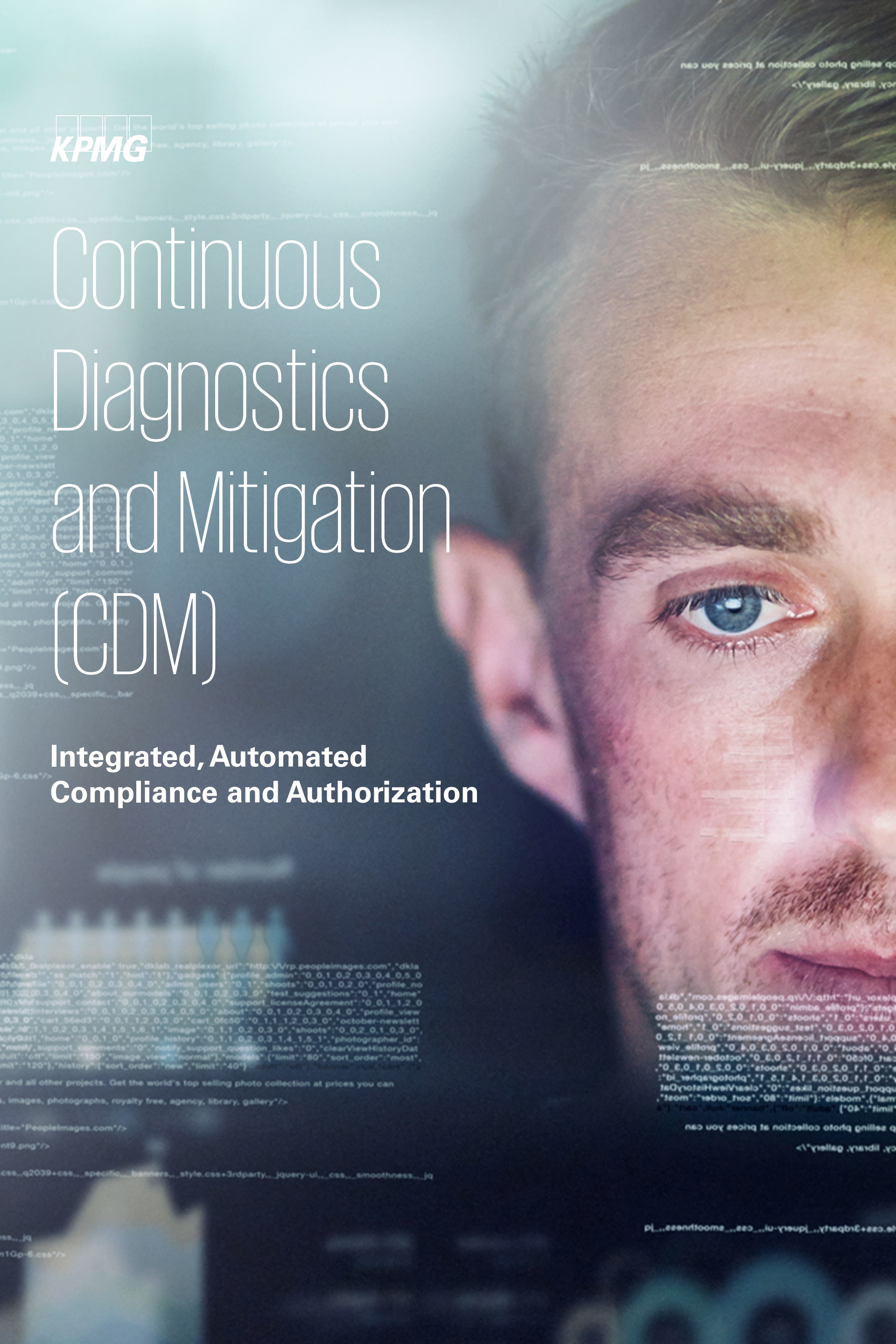


KPMG

Continuous Diagnostics and Mitigation (CDM)

Integrated, Automated Compliance and Authorization

Overview

- Congress established the Continuous Diagnostics and Mitigation (CDM) program to provide adequate, risk-based, and cost-effective cybersecurity and more efficiently allocate cybersecurity resources. CDM 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.

- The CDM program is a dynamic approach to fortifying the cybersecurity of Government networks and systems. The cyber landscape in which Federal Agencies operate is constantly changing and dynamic. Similarly, threats to the nation's information security continue to evolve and Government leaders recognize the need for a modified approach to protecting our cyber infrastructure. The Government’s CDM Program helps enable the Department of Homeland Security (DHS) , as executive agent, along with Federal Agencies and state, local, regional, and tribal governments, with the ability to enhance and further automate their existing continuous network monitoring capabilities, correlate and analyze critical cybersecurity-related information, and enhance risk-based decision making at the Agency and Federal enterprise level. The CDM Program benefits participating Agencies by helping to identify information security risks on an ongoing basis so that Agencies can rapidly detect and respond to information security events.

- Many Government agencies have found that the DHS-contracted assistance from several system integrators have been lacking. These agencies have looked for assistance from KPMG to provide talent beyond equipment installation and proprietary integrations.

CDM services

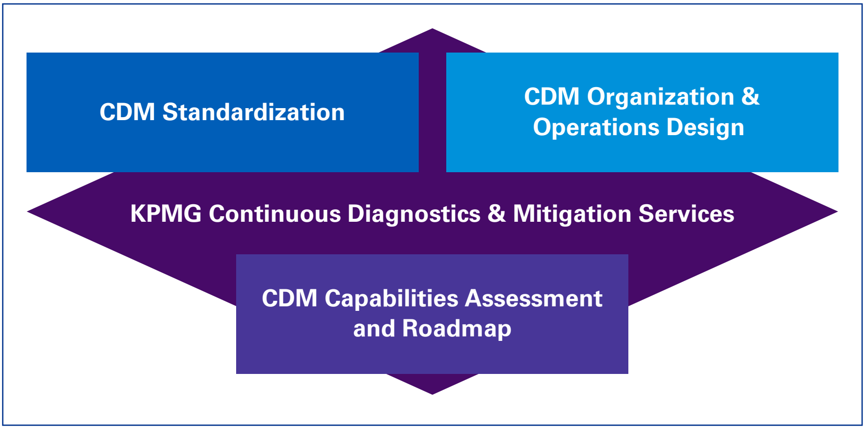
KPMG Continuous Diagnostics and Mitigation (CDM) services deliver integration and architecture support to assist Federal Agencies in realizing value and achieving the goal of continuous compliance and authorization from their investments in CDM.

KPMG provides five (5) types of CDM services across all Phases of CDM

1. **CDM Integration Support** provides assistance to agencies in onboarding their data into the CDM Integration platform. The service also provides data model customization and onboarding of data from CDM Layer1 sensors.
2. **CDM Architecture Optimization** provides CDM architecture and capabilities assessment to allow agencies to more efficiently capture and process data provided by the CDM sensor layer. KPMG develops an actionable series of improvement steps in a CDM Roadmap to guide Agency investment and training strategies.
3. **Remediation Automation Support** provides assistance to agencies seeking to increase their degree of automation when remediating non-compliant systems detected through CDM. The service helps Agencies develop automated workflows within ticketing systems and automated endpoint management systems.
4. **Data Visualization Support** provides requirements identification, CDM metrics development, and dashboard creation to deliver actionable risk intelligence to Agency and Federal CDM dashboards. The service provides assistance with development of an agency risk score developed from measurement and compilation of individual system risk scores.
5. **Ongoing Authorization Support** provides assistance to Agency CIOs in developing, implementing, or maturing an Ongoing Authorization capability based on their CDM program. The service springboards off successful measurement of risk within each system through computation of system risk scores and tracks development and maintenance of Body of Evidence artifacts supporting system authorization decisions.

KPMG approach

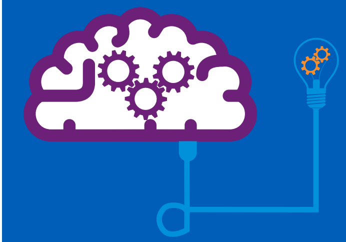
KPMG CDM Service delivery approach offers three (3) areas of focus to assist our clients. These include assessment of CDM architecture, establishment of an architecture organization, and development of security architecture design.


CDM Standardization
CDM Organization & Operations Design
KPMG Continuous Diagnostics & Mitigation Services
CDM Capabilities Assessment and Roadmap

- ***CDM Capabilities Assessment and Roadmap:*** The assessment provides the foundation for all of our CDM services. The objective is to develop an initial understanding of an organization's current state of CDM capabilities. KPMG identifies key operations and personnel drivers, conducts a deep-dive of the current sensor solutions, data integration status and installed data models, and CDM performance metrics. KPMG performs a gap analysis and provides actionable recommendations to improve the effectiveness of the Agency CDM program in the form of a CDM Roadmap. The roadmap aligns business objectives, training and investment strategies to implement the future state CDM capability, while offering clients the opportunity for knowledge transfer.

KPMG approach (continued)

- ***CDM Organization & Operations Design:*** The objective is to define CDM organizational capabilities – more specifically the capabilities of the staff assigned to operate Agency CDM. During this phase KPMG will review current CDM organization capabilities, personnel training and chain(s) of command. We also review current processes and procedures followed by the CDM organization. KPMG assists the client with establishing a CDM Governance model and creates/ updates processes for the Security Architecture organization. KPMG has the ability to provide assistance with implementation of an Enterprise Security Architecture artifacts tracking tool.
- ***CDM Standardization:*** Spring-boarding from the CDM assessment, the objective is to develop an Agency-wide standardized CDM technology stack and data models supporting data collection, risk scoring, and sub-agency reporting of operational risk to an Agency.



KPMG begins each CDM engagement with an assessment of the current state of the capability at the client to better understand their needs. The assessment provides a snapshot of the maturity level of people, technology, and procedures supporting CDM. The results of this assessment allow KPMG to leverage appropriate resources and skill mix.

Client challenges

Today many Government organizations face a common set of challenges and roadblocks in operationalizing CDM:

1. Lack of personnel trained in cyber security disciplines
2. Lack of personnel trained in elements of the CDM technology stack
3. Lack of applied technical guidance and expertise in implementing the CDM technology stack
4. CDM solutions cross several lines of responsibility without a clear leader or organizational leadership support
5. Ineffective or spotty support from CDM DEFEND integrators
6. Inconsistently implemented CDM architecture and security solutions covering hybrid and cloud-native systems
7. Lack of clarity of vision or roadmap to operationalizing CDM
8. Limited or no standardization among lead agency and subordinate agencies
9. Existence of "shadow IT" stemming from organizational reluctance
10. Inability to standardize or leverage knowledge from previous security projects.

CDM service drivers

Some of the drivers to develop a standardized security architecture for any organization include:

- ***Changing Threat Landscape*** drives the CDM Architecture to improve Security based on new threats and information provided by threat feeds.
- ***Standardization*** drives each Agency to standardize their CDM technology stack and data architectures to more effectively integrate sub-agency data flows and provide a coherent, actionable picture of risk to Agency decision-makers and the Federal Dashboard
- ***Evolving Technologies*** drives architects to always look to improve agency security posture with infusion new and ever-changing technologies and capabilities.
- ***Legal and Regulatory Requirements*** demand a structured, effective CDM architecture to address security needs based on Federal mandates.
- ***Business Requirements*** motivate Security Architecture in meeting business technical security needs.
- ***Risk Management and Compliance*** promotes the need for a structured, well-integrated CDM Data and technology Architecture that delivers actionable steps to effectively manage and mitigate IT security risks.

Benefits and outcomes

Potential client benefits by adopting a standardized/ structured CDM data architecture framework:

01 Better risk management decisions, strategically aligned with business goals

02 Value-added spend on cyber security

03 Better CDM technology integration with enterprise architecture

04 More effective protection from cyber attacks

05 Continuous monitoring and scoring of security risk

06 Risk-focused security strategy

07 Auditable compliance

08 Ongoing Authorization support

09 Consistent CDM data flow to Agency and Federal Dashboards

Conclusion

A successful CDM program delivers more than statistics presented on a dashboard – it provides the necessary decision tools to help enable Agency stakeholders make informed, risk-based decisions. KPMG's CDM services facilitate success through knowledge transfer, auditable compliance and a CDM roadmap aligned with the Agency's business objectives.

Notes

Notes

KPMG

Contacts

If you have questions or want more details regarding KPMG's CDM services, please contact us:

Tony Hubbard
Principal, Advisory
T: 703-286-8320
E: thubbard@kpmg.com

Sallie Sweeney
Director, Advisory
T: 703-286-8000
E: salliesweeney@kpmg.com

Shane Cashdollar
Director, Advisory
T: 703-286-8236
E: scashdollar@kpmg.com

Joe Faraone
Director, Advisory
T: 703-286-8000
E: jfaraone@kpmg.com

kpmg.com/socialmedia

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.