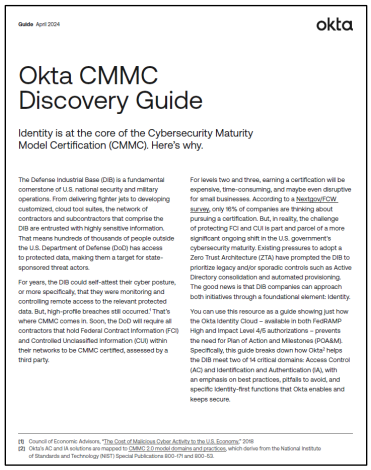

Guide April 2024 okta

Okta CMMC Discovery Guide

Identity is at the core of the Cybersecurity Maturity Model Certification (CMMC). Here's why.

The Defense Industrial Base (DIB) is a fundamental cornerstone of U.S. national security and military operations. From delivering fighter jets to developing customized, cloud tool suites, the network of contractors and subcontractors that comprise the DIB are entrusted with highly sensitive information. That means hundreds of thousands of people outside the U.S. Department of Defense (DoD) has access to protected data, making them a target for state-sponsored threat actors.

For years, the DIB could self-attest their cyber posture, or more specifically, that they were monitoring and controlling remote access to the relevant protected data. But, high-profile breaches still occurred.[1] That's where CMMC comes in. Soon, the DoD will require all contractors that hold Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their networks to be CMMC certified, assessed by a third party.

For levels two and three, earning a certification will be expensive, time-consuming, and maybe even disruptive for small businesses. According to a NextGovFCW survey, only 16% of companies are thinking about pursuing a certification. But, in reality, the challenge of protecting FCI and CUI is part and parcel of a more significant ongoing shift in the U.S. government's cybersecurity maturity. Existing pressures to adopt a Zero Trust Architecture (ZTA) have prompted the DIB to prioritize legacy and/or sporadic controls such as Active Directory consolidation and automated provisioning. The good news is that DIB companies can approach both initiatives through a foundational element: Identity.

You can use this resource as a guide showing just how the Okta Identity Cloud – available in both FedRAMP High and Impact Level 4/5 authorizations – prevents the need for Plan of Action and Milestones (POA&M). Specifically, this guide breaks down how Okta[2] helps the DIB meet two of 14 critical domains: Access Control (AC) and Identification and Authentication (IA), with an emphasis on best practices, pitfalls to avoid, and specific identity-first functions that Okta enables and keeps secure.

(1) Council of Economic Advisers, "The Cost of Malicious Cyber Activity to the U.S. Economy," 2018
(2) Okta's AC and IA solutions are mapped to CMMC 2.0 model domains and practices, which derive from the National Institute of Standards and Technology (NIST) Special Publications 800-171 and 800-53.

Okta CMMC Discovery Guide

Identity is at the core of the Cybersecurity Maturity Model Certification (CMMC). Here's why.

Thank you for downloading this Okta Discovery Guide. Carahsoft is the distributor for Okta Cybersecurity solutions available via GSA, NASA-SEWP, ITES-Sw2, DoD ESI and other contract vehicles.

To learn how to take the next step toward acquiring Okta's solutions, please check out the following resources and information:

For additional resources:
carah.io/resources

For upcoming events:
carah.io/events

For additional Okta solutions:
carah.io/solutions

For additional Cybersecurity solutions:
carah.io/cybersecurity

To set up a meeting:
okta@carahsoft.com
833-674-3990

To purchase, check out the contract vehicles available for procurement:
carah.io/contracts

For more information, contact Carahsoft or our reseller partners:
okta@carahsoft.com | 833-674-3990

okta

Okta CMMC Discovery Guide

Identity is at the core of the Cybersecurity Maturity Model Certification (CMMC). Here's why.

The Defense Industrial Base (DIB) is a fundamental cornerstone of U.S. national security and military operations. From delivering fighter jets to developing customized, cloud tool suites, the network of contractors and subcontractors that comprise the DIB are entrusted with highly sensitive information. That means hundreds of thousands of people outside the U.S. Department of Defense (DoD) has access to protected data, making them a target for state-sponsored threat actors.

For years, the DIB could self-attest their cyber posture, or more specifically, that they were monitoring and controlling remote access to the relevant protected data. But, high-profile breaches still occurred.[1] That's where CMMC comes in. Soon, the DoD will require all contractors that hold Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) within their networks to be CMMC certified, assessed by a third party.

For levels two and three, earning a certification will be expensive, time-consuming, and maybe even disruptive for small businesses. According to a Nextgov/FCW survey, only 16% of companies are thinking about pursuing a certification. But, in reality, the challenge of protecting FCI and CUI is part and parcel of a more significant ongoing shift in the U.S. government's cybersecurity maturity. Existing pressures to adopt a Zero Trust Architecture (ZTA) have prompted the DIB to prioritize legacy and/or sporadic controls such as Active Directory consolidation and automated provisioning. The good news is that DIB companies can approach both initiatives through a foundational element: Identity.

You can use this resource as a guide showing just how the Okta Identity Cloud – available in both FedRAMP High and Impact Level 4/5 authorizations – prevents the need for Plan of Action and Milestones (POA&M). Specifically, this guide breaks down how Okta[2] helps the DIB meet two of 14 critical domains: Access Control (AC) and Identification and Authentication (IA), with an emphasis on best practices, pitfalls to avoid, and specific Identity-first functions that Okta enables and keeps secure.

---

[1] Council of Economic Advisors, "The Cost of Malicious Cyber Activity to the U.S. Economy," 2018

[2] Okta's AC and IA solutions are mapped to CMMC 2.0 model domains and practices, which derive from the National Institute of Standards and Technology (NIST) Special Publications 800-171 and 800-53.

okta

Figure 1 – CMMC Control Graph Mapped

Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)
AC.L1-3.1.1	AT.L2-3.2.1	AU.L2-3.3.1	CM.L2-3.4.1	IA.L1-3.5.1	IR.L2-3.6.1	MA.L2-3.7.1
AC.L1-3.1.2	AT.L2-3.2.2	AU.L2-3.3.2	CM.L2-3.4.2	IA.L1-3.5.2	IR.L2-3.6.2	MA.L2-3.7.2
AC.L2-3.1.3	AT.L2-3.2.3	AU.L2-3.3.3	CM.L2-3.4.3	IA.L2-3.5.3	IR.L2-3.6.3	MA.L2-3.7.3
AC.L2-3.1.4		AU.L2-3.3.4	CM.L2-3.4.4	IA.L2-3.5.4		MA.L2-3.7.4
AC.L2-3.1.5		AU.L2-3.3.5	CM.L2-3.4.5	IA.L2-3.5.5		MA.L2-3.7.5
AC.L2-3.1.6		AU.L2-3.3.6	CM.L2-3.4.6	IA.L2-3.5.6		MA.L2-3.7.6
AC.L2-3.1.7		AU.L2-3.3.7	CM.L2-3.4.7	IA.L2-3.5.7		
AC.L2-3.1.8		AU.L2-3.3.8	CM.L2-3.4.8	IA.L2-3.5.8		
AC.L2-3.1.9		AU.L2-3.3.9	CM.L2-3.4.9	IA.L2-3.5.9		
AC.L2-3.1.10				IA.L2-3.5.10		
AC.L2-3.1.11				IA.L2-3.5.11		
AC.L2-3.1.12						
AC.L2-3.1.13						
AC.L2-3.1.14						
AC.L2-3.1.15						
AC.L2-3.1.16						
AC.L2-3.1.17						
AC.L2-3.1.18						
AC.L2-3.1.19						
AC.L1-3.1.20						
AC.L2-3.1.21						
AC.L1-3.1.22						

Meets CMMC 2.0 Control | Supports CMMC 2.0 Control | N/A | Primary Service | Secondary Service | Level 1 Requirement

okta

Figure 2 – CMMC Control Graph Mapped cont.

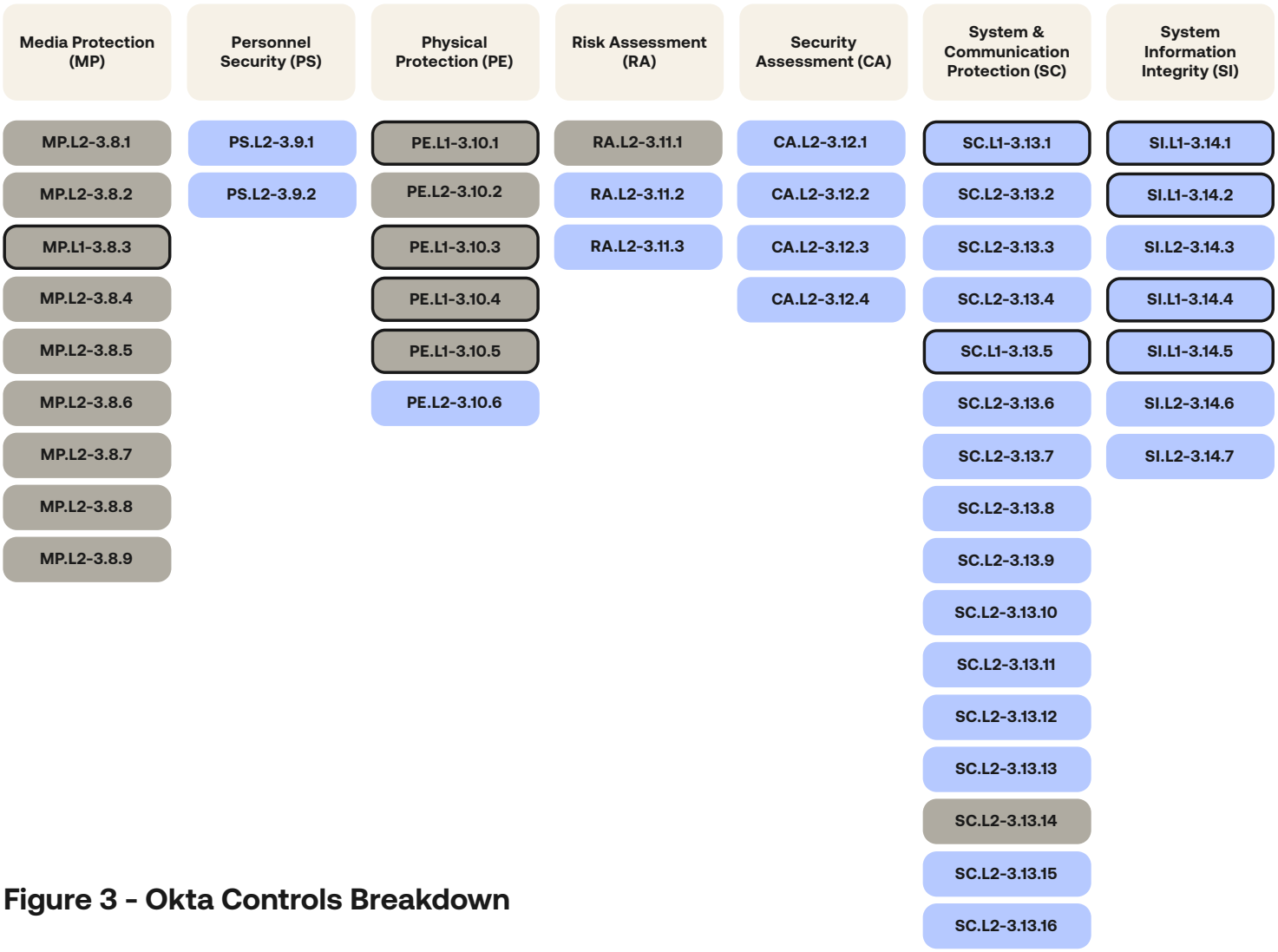

Figure 3 - Okta Controls Breakdown

CMMC Level	L1	L2
Okta supported controls	10	80
All technical controls	17	110
% of controls supported by Okta	59%	73%

Meets CMMC 2.0 Control | Supports CMMC 2.0 Control | N/A | Primary Service | Secondary Service | Level 1 Requirement

okta

CMMC Domain: Access Control (AC)

What to know

This CMMC domain emphasizes the importance of not only basic access control functions but also enhanced security measures such as defaulting to least-privileged access — using context from across the entire security stack — and automatically terminating a user's session after defined conditions. Failure to meet these Zero Trust-informed guidelines exposes FCI and CUI to risks related to weak access control measures, poor credential management, and system vulnerabilities.

Pitfalls to avoid

Access control measures must avoid granting blanket access that fails to delineate appropriate role- and function-specific access levels. Often, these oversights trace back to siloed user databases that don't provide a full view of each user's level of access. From a user experience perspective, DIB companies must also steer clear of difficult-to-navigate processes for common problems like session timeout and reauthentication.

The Okta advantage

- **Lifecycle Entitlement Management:** Ensures least-privilege access and deprovisioning through a set of customizable, centrally managed policies.
- **Access Visibility:** Offers administrators a risk-appropriate, continuously-adaptive view of which users have access to which applications — and logs administrative actions.
- **IT Admin Management:** Enables administrators to manage session timeout, lock out, and reauthentication processes based on individual policy.
- **Easy Integration with VPN, Remote Access, and Secure Shell:** Allows secure access remotely — and appropriately controlled and monitored.
- **Privacy Protections:** Prevents unnecessary data collection without consent and ensures collection is in accordance with applicable regulations.

What to read next

- Okta Identity Governance: A SaaS-delivered, converged, and intuitive IAM platform
- Okta Device Access: Extends IAM capabilities across devices and apps, protecting your org from phishing attacks
- Okta Privileged Access: Mitigates the risk of authorized access to resources

okta

CMMC Domain: Identification and Authentication (IA)

What to know

The CMMC model underscores the urgency of employing multi-factor authentication (MFA) as a core means of protecting FCI and CUI from phishing attacks. Without strong IA, DIB companies attract risk with abandoned credentials that have not been revoked by administrators or an automated system.

Pitfalls to avoid

DIB companies must avoid inadequate MFA methods (e.g push notifications) that fail to meet minimum phishing-resistant standards. By practicing good password hygiene (e.g., stop relying on passwords in general, forbidding the reuse of credentials, and mandating and automating credential updates) they can also avoid leaving login credentials vulnerable to misuse and strive for passwordless, phishing-resistant MFA in every place possible.

The Okta advantage

- **Identity-Led Security Framework:** Verifies and manages users accessing sensitive information within flexible, organization-specific parameters.
- **Centralized Management Console:** Allows admins to implement, enforce, and adjust password rules and schedules in accordance with government compliance requirements.
- **Adaptive MFA:** Delivers step-up authentication for higher-risk applications, providing contextual access using a variety of customizable factors including one-time passwords, app-based verification, physical tokens, and more.

What to read next

- Okta MFA: Ability to add authenticators with different factor types and method characteristics
- Okta Adaptive MFA: Uses a broad set of modern factors, leverages insight from millions of users, devices, and authentications, and integrates easily with your apps and network infrastructure
- Okta FastPass: Provides passwordless authentication to any SAML, OIDC, or WS-Fed app in Okta

Okta has a history of supporting DIB companies through the ever-evolving journey of federal compliance standards. Whether your company supports the DoD in an operational, technical, manufacturing, or research capacity, Okta's unique consultative approach will help personalize robust, CMMC-compliant Identity and Access Management to your organization's specific needs. We've seen mostly everything, we know the common pitfalls, and we can help your IT, governance, and oversight programs lead the company to a secure and collaborative culture, all while strengthening your DoD relationship.