citrix™ | Public Sector

How Citrix can help you achieve CMMC certification

Achieving CMMC certification can be a daunting task for any contractor. Fortunately, Citrix is here to help. Security solutions from Citrix can help you to implement dozens of processes across thirteen of the seventeen CMMC domains.

Security solutions from Citrix provide a comprehensive set of policy enforcement, security analytics, and risk management capabilities to greatly simplify and expedite the CMMC certification process. Citrix solutions are easy to implement, comprehensive in scope, flexible in design, and scalable to support large complex enterprise environments spanning on-premises and hybrid multi-cloud. As part of a larger security ecosystem, Citrix security solutions also integrate with leading third-party solutions such as Splunk and Microsoft Intune.

What is CMMC?

The Cybersecurity Maturity Model Certification (CMMC) is a new standard for cybersecurity implementation and certification for Aerospace and Defense contractors across the Defense Industrial Base (DIB) sector. It is intended to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) processed or held by contractors and subcontractors by requiring the adoption and implementation of standardized cybersecurity processes and practices. The CMMC framework enables contractors to measure and certify their cybersecurity maturity against a progressive model of five levels.

Levels	Process	Practices
5	Optimizing	Advanced / Progressive
4	Reviewed	Proactive
3	Managed	Good Cyber Hygiene
2	Documented	Intermediate Cyber Hygiene
1	Performed	Basic Cyber Hygiene

Each CMMC maturity level is cumulative, so achievement of a specific level also requires achievement of all preceding lower levels. The processes and practices within CMMC fall under a set of seventeen domains originating from FIPS Publication 200:

- Access Control (AC)
- Asset Management (AM)
- Audit and Accountability (AU)
- Awareness and Training (AT)
- Configuration Management (CM)
- Identification and Authentication (IA)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Personnel Security (PS)
- Physical Protection (PE)
- Recovery (RE)
- Risk Management (RM)
- Security Assessment (CA)
- Situational Awareness (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

The challenges of CMMC certification

Unlike its predecessor (DFARS 252.204-7012), CMMC includes a verification component whereby designated CMMC Third Party Assessment Organizations (C3PAOs) will conduct assessments to ensure contractors are compliant and will grant certification at a specific maturity level. Certification is required for all contractors and subcontractors along a contract's supply chain.

CMMC certification is scheduled to be required for all DoD contracts by 2025. However, DoD is in the process of phasing in the CMMC certification requirement on selected contracts in the preceding years. Achieving CMMC certification will require a significant investment in both effort and budget for large DoD contractors, especially at higher maturity levels. Also unlike preceding regulations, CMMC certification must be achieved prior to the contract award date rather than the period of performance start date. For these reasons, DoD contractors should be actively working on preparing for CMMC certification now.

Preparing for CMMC certification means adopting all of the necessary processes and practices included in the desired maturity level. However, simply adopting the processes and practices isn't necessarily sufficient to be eligible for certification. Processes must be institutionalized, meaning they are embedded and ingrained in the organization to ensure that they are followed consistently and reliably. Practices must be implemented at the same level of maturity as the processes.

The DoD has made clear that a failure to achieve CMMC certification will exclude contractors from being considered for contracts, and this extends down to all subcontractors as well. This translates into serious financial risk for contractors who fail to achieve certification or fail to achieve the required maturity level for a desired contract.

The following table maps security solutions from Citrix and the CMMC process domains which they can implement.

Solution	Domain																
	AC	AM	AU	AT	CM	IA	IR	MA	MP	PS	PE	RE	RM	CA	SA	SC	SI
ADC/CWAAP	✓					✓		✓				✓	✓			✓	✓
Analytics for Security			✓				✓						✓	✓	✓		✓
Application Delivery Management			✓		✓		✓						✓	✓	✓		✓
Endpoint Management	✓	✓			✓	✓										✓	✓
Secure Internet Access	✓															✓	✓
Secure Workspace Access	✓																
Virtual Apps and Desktops	✓						✓	✓								✓	
Wrike					✓												

Citrix Solution Descriptions

ADC/Web Application and API Protection (CWAAP): Citrix ADC and Web Application and API Protection are the most comprehensive application delivery, load balancing, and application security solutions for both monolithic and microservices-based applications. ADC and CWAAP provide web application (layer 7) firewalling, bot management, DDoS management, API protection, and other layer 3-7 security protections with an easy to manage interface and hybrid multi-cloud platform support.

Analytics for Security (CAS): Citrix Analytics for Security provides user behavior analysis and risk mitigation by leveraging AI and Machine Learning. Analytics builds behavioral models for each user and continuously monitors subsequent behavior against the model, computing a risk score based on how atypical a user's behavior is. Users engaged in risky behavior can trigger closed-loop autonomous actions (such as initiating session recording or blocking access) to reduce risk and prevent potential data loss or breach.

Application Delivery Management (CADM): Citrix ADM delivers actionable insights across on-premises and multi-cloud environments by providing centralized management, provisioning, and orchestration of Citrix ADC and SD-WAN deployments. ADM detects and correlates security threats across multiple networks to provide comprehensive visibility into enterprise-wide risk and security posture.

Endpoint Management (CEM): Citrix Endpoint Management combines unified endpoint management features with extensive security and contextual access policies to secure end user devices and enforce a zero-trust network architecture. CEM also includes industry-leading secure mobile apps for email, intranet browsing, and file viewing/editing to provide a secure containerized for offline mobile user experience.

Secure Internet Access (CSIA): Citrix Secure Internet Access provides a comprehensive stack to secure Internet traffic across the enterprise, combining all of the features of a Secure Access Service Edge (SASE) including a secure web gateway firewall, cloud access security broker (CASB), malware protection, data loss prevention (DLP), and traffic sandboxing. CSIA uses a single-pass architecture and hundreds of points of presence across the world to provide scalability to service the largest enterprises without impacting network performance or application responsiveness.

Secure Workspace Access (CSWA): Citrix Secure Workspace Access provides secure access to internal apps and intranet sites utilizing a zero-trust approach regardless of where your users reside. CSWA doesn't require difficult-to-manage VPN client infrastructure, and instead leverages secure TLS tunneling to provide VPN-less access that greatly simplifies the remote user experience while enforcing enterprise security policies and complying with industry regulations.

Virtual Apps and Desktops (CVAD): Citrix Virtual Apps and Desktops is the industry leader in delivering virtual desktops and applications across hybrid multi-cloud environments. CVAD enables customers to implement a zero-residual data architecture to prevent data leakage outside of a security authorization boundary.

Wrike: Wrike provides collaborative work management (CWM) and product and portfolio management (PPM) capabilities via an easy-to-use, commercial-like user interface that greatly simplifies project, task, and resource management activities across multiple programs. Wrike includes comprehensive reporting and analysis for business and project-oriented metrics to maximize project success and measure risk.

Learn More

To schedule a discussion on how Citrix can help you achieve your CMMC certification, contact the Citrix Federal Systems Integrator team:

Adam Savoy
610.850.5969
adam.savoy@citrix.com

Rob Persinger
703.216.2519
robert.persinger@citrix.com

Matt Porco
703.431.3153
matt.porco@citrix.com

citrix | Public Sector

US Public Sector Sales
1-800-424-8749 x26603 | https://www.citrix.com/solutions/government/

Locations
Corporate Headquarters | 851 Cypress Creek Road, Fort Lauderdale, FL 33309, United States
US Public Sector Offices | 7735 Old Georgetown Road, Suite 300, Bethesda, MD 20814, United States