Google Workspace

Achieve CMMC compliance with Google Workspace

Contents

- **Executive Summary** 03
- **Background to CMMC** 04
  - What is the purpose of CMMC?
  - Impact to DoD contractors
- **Workspace Can Be Your Foundation to CMMC Compliance** 05
- **Secure Data Management** 07
  - Encrypting CUI in transit and at rest
  - Data Loss Prevention
  - Vendor Access Control
- **Enhanced Cybersecurity** 11
  - Multi-Factor Authentication
  - Passkeys
- **Proven Compliance Credentials** 13
  - Certifications and audits
  - Independent third-party attestations
- **Scalable solutions** 15
  - Government-grade commercial cloud
- **Establishing a security-first culture with Workspace** 17
- **How Workspace can help** 18

❤️ 12 ✌️ 24

Executive Summary

In the wake of upcoming mandatory adherence to new CMMC requirements, Google Workspace can help Defense Industrial Base organizations proactively support compliance at a significantly lower cost.

The Cybersecurity Maturity Model Certification (CMMC) is a unified framework for implementing cybersecurity across the Defense Industrial Base (DIB), federal contractors and subcontractors and technology providers. It ensures that Organizations Seeking Certification (OSCs) can securely process and store Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). In other words, the goal of CMMC is to protect sensitive information and ensure that industry meets cybersecurity requirements.

- To achieve this, CMMC integrates the security controls outlined in NIST Special Publication 800-171, along with additional requirements specific to the CMMC framework.
- CMMC requirements are rolling out with a phased approach. The requirement for compliance with CMMC Level 1 and 2 self assessments may start now, while Level 2 C3PAO and Level 3 assessments will be included in Department of Defense DoD contracts over the next 3 years.
- For DIB organizations eager to complete their CMMC assessment ahead of contractual requirements, Level 1 and 2 self assessments, and Level 2 C3PAO assessments may start now.

Google Workspace with the Assured Controls Plus add-on can support organizations to meet CMMC requirements needed for email, calendar, document repository, video conferencing, chat, collaboration, eDiscovery, archiving, and more. This is offered at a **significantly lower cost** than traditional vendors offering alternative solutions and is **FedRAMP High and IL4 authorized.**

Workspace runs on a single cloud environment eliminating the need for a separate government cloud. We believe that the traditional government cloud approach presents challenges with resilience and pace of innovation. In contrast, Workspace has been designed to serve the public sector and government agencies without the drawbacks of traditional solutions.

Workspace also offers public sector organizations comprehensive migration support including possible subsidies for migration costs, dedicated assistance, specialized tools, and a network of expert partners.

Please note: *This whitepaper applies to Google Cloud products described at workspace.google.com and cloud.google.com and is current as of February 2025 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers. Organizations should seek independent legal advice relating to their responsibilities under CMMC. Nothing in this document is intended to provide or be used as a substitute for legal advice.*

Background to CMMC

What is the purpose of the CMMC?

As a result of growing cybersecurity concerns around the theft of intellectual property and sensitive information, the U.S. Department of Defense (DoD) created the Cybersecurity Maturity Model Certification (CMMC) 2.0; a top-tier standard used to assess and enhance the cybersecurity posture of contractors who serve the DoD.

Impact to DoD contractors

For defense contractors and supply chain companies working with the Department of Defense (DoD), compliance is not an option—certification is a required business baseline to progress contracts and renewals.

Workspace can help organizations meet the steep requirements of CMMC 2.0 compliance through its cloud-based solution that includes robust security features.

❤️ 12 ✌️ 24

Workspace can be the foundation to your **CMMC Compliance**

Key benefits of Workspace for CMMC 2.0

Workspace provides more than just productivity tools—it is a trusted partner in helping navigate the complex world of CMMC 2.0 compliance. With its AI-assisted security controls combined with a commitment to ongoing compliance efforts, organizations can confidently protect sensitive government data while maintaining a strong cybersecurity posture.

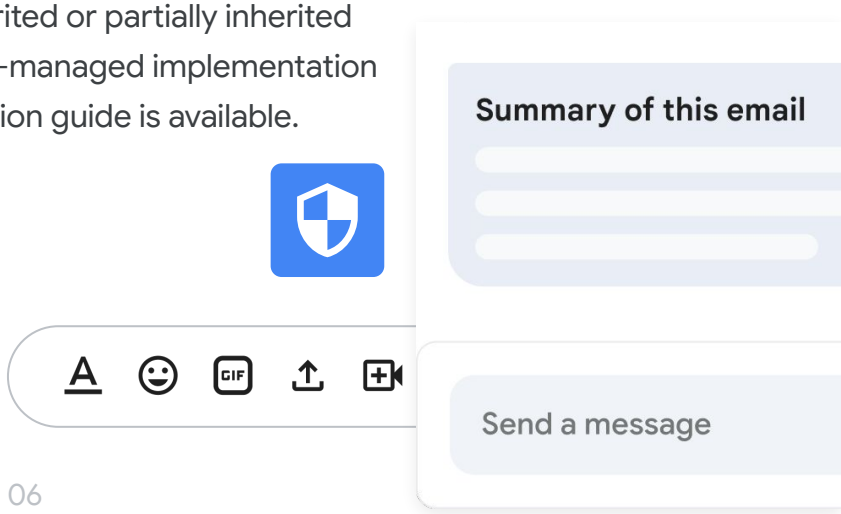
Secure Data Management
Encryption, Data Loss Prevention (DLP) and access control for Controlled Unclassified Information (CUI) protection.

Proven Compliance Credentials
Certifications and audits (ISO, SOC, FedRAMP, etc.) demonstrate Google's commitment to security standards.

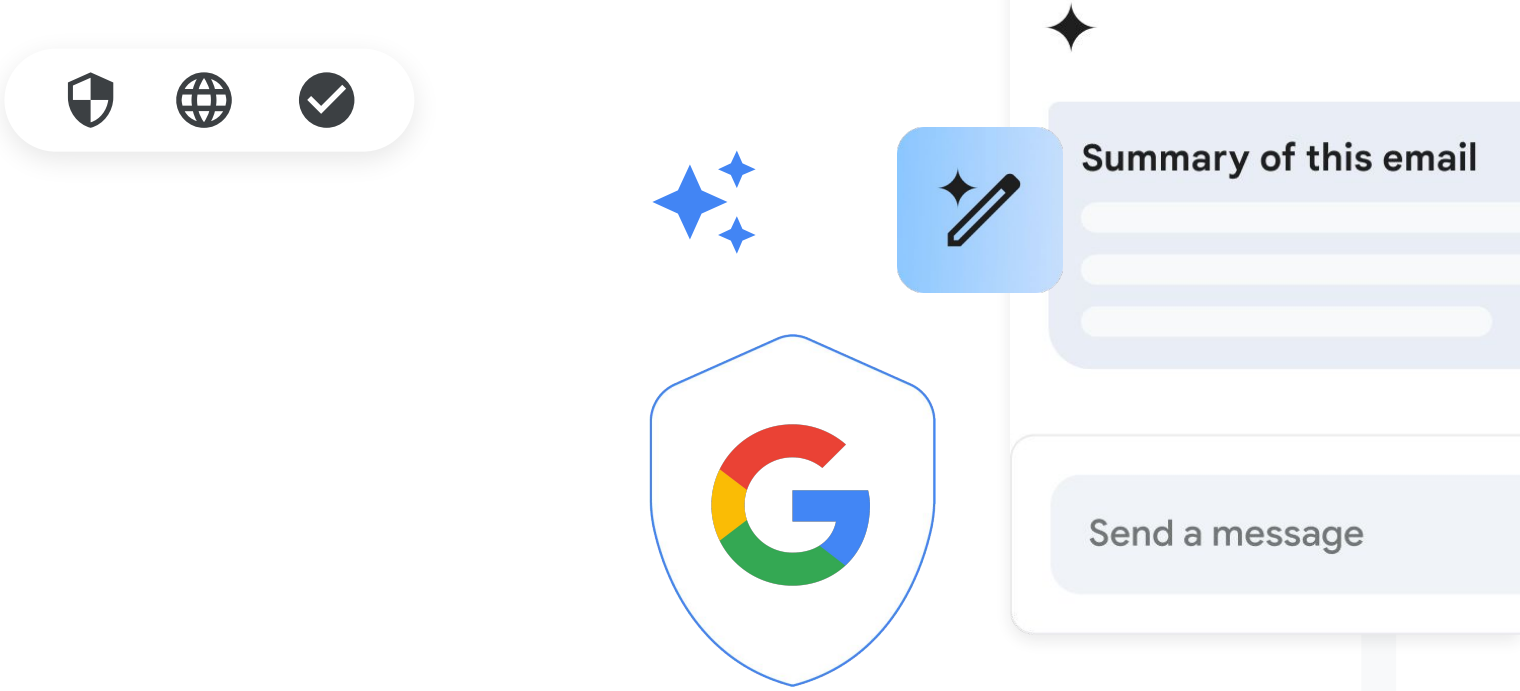
Enhanced Cybersecurity
Industry leading features such as multi-factor authentication and phishing protection.

Scalable Solutions
A cloud-based infrastructure that meets the needs of your organization and adapts to the evolving needs of your organization.

Successfully meeting CMMC 2.0 compliance is a shared responsibility between the technology provider and customer. Some controls are inherited or partially inherited from Google Workspace and require customer-managed implementation and verification. A comprehensive implementation guide is available.



Secure Data **Management**



Encrypting CUI in transit and at rest

Workspace helps customers to secure Controlled Unclassified Information (CUI) with encryption both in transit and at rest, per CMMC AC.L2-3.1.19.

What is encryption?

Encryption is an important piece of the Workspace security strategy, helping to protect emails, chats, video meetings, files, and other data.

First, we encrypt certain data as described below while it is stored "at rest"—stored on a disk (including solid-state drives) or backup media. Even if an attacker or someone with physical access obtains the storage equipment containing your data, they won't be able to read it because they don't have the necessary encryption keys. Second, we encrypt all customer data while it is "in transit"—traveling over the Internet and across the Google network between data centers. Should an attacker intercept such transmissions, they will only be able to capture encrypted data. We'll take a detailed look at how we encrypt data stored at rest and data in transit below.

Google has led the industry in using Transport Layer Security (TLS) for email routing, which allows Google and non-Google servers to communicate in an encrypted manner and is required for CMMC SC.L1-3.13.1. When you send email from Google to a non-Google server that supports TLS, the traffic will be encrypted, preventing passive eavesdropping. We believe increased adoption of TLS is so important for the industry that we report TLS progress in our Email Encryption Transparency Report.

We also improved email security in transit by developing and supporting the MTA Strict Transport Security (MTA-STS) standard allowing receiving domains to require transport confidentiality and integrity protection for emails. Workspace customers also have the extra ability to only permit email to be transmitted to specific domains and email addresses if those domains and addresses are covered by TLS. This can be managed through the TLS compliance setting.

Client-side encryption

For an additional layer of confidentiality to protect organizations' most sensitive data, client-side encryption (CSE) is a state-of-the-art privacy-preserving technology that allows the customer to be the sole arbiter of their data. Client-side encryption takes Google's existing encryption capability to the next level by ensuring that customers have sole control over their encryption keys, and using Secure/Multipurpose Internet Mail Extensions (S/MIME) to prevent unauthorized access of data during transmission, as required for CMMC SC.L2-3.13.8.

Data Loss Prevention (DLP)

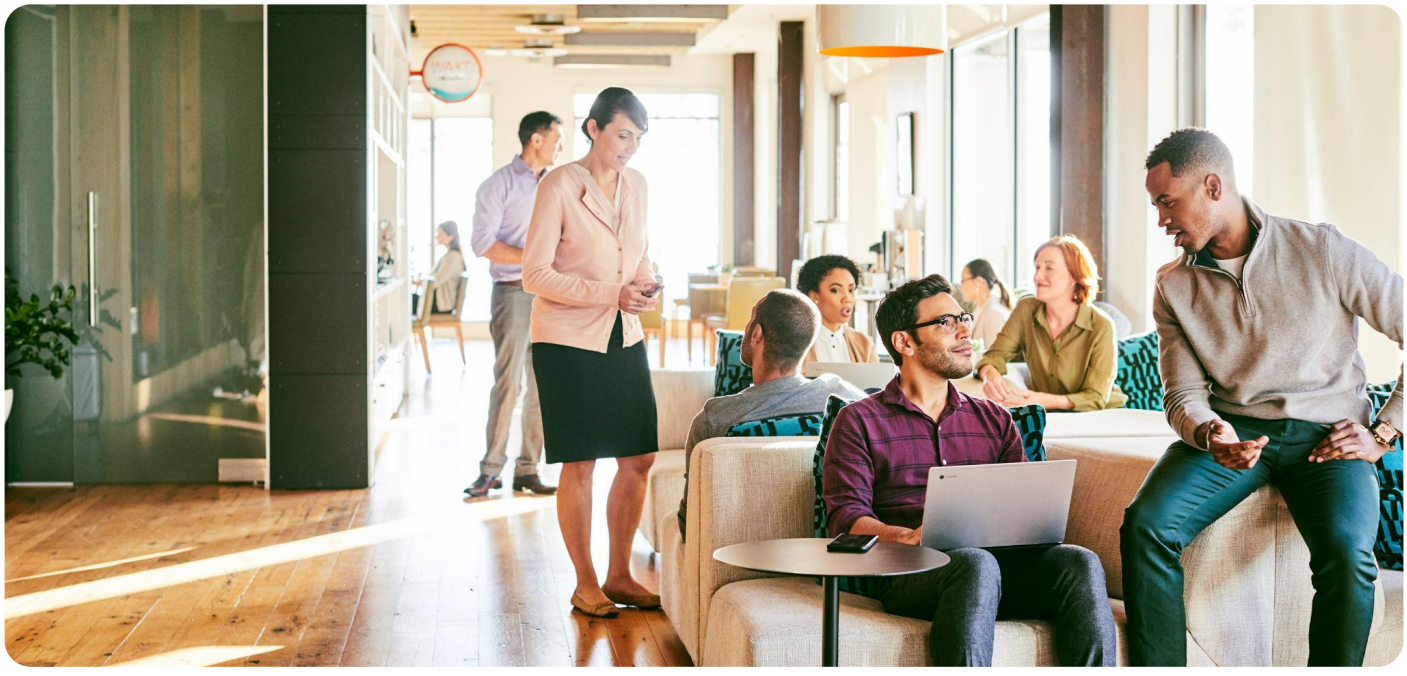
Data loss prevention (DLP), which aligns with CMMC AC.L2-3.1.3, adds another layer of protection designed to help prevent CUI, sensitive or private information such as payment card numbers, national identification numbers, or protected health information, from leaking outside of an organization.

DLP enables customers to audit how sensitive data is flowing in their enterprise and turn on warning or blocking actions to help prevent users from either accidentally or maliciously sending confidential data.

To enable this, DLP provides over 100 predefined content detectors, including detection of global and regional identifiers, medical information, and credentials. Customers can also define their own custom detectors to meet their needs, or integrate DLP with the AI classification capabilities within Workspace, to automatically identify and label sensitive information based on their unique data class definitions, then enforce access rules based upon the label-based DLP.

For greater control over which users and devices can transfer sensitive content, DLP rules can be combined with Context-Aware Access conditions, such as user location, device security status (managed, encrypted) and IP address. When you add a Context-Aware Access policy to a DLP rule, the rule is enforced only if the context conditions are met.

For attachments and image-based documents, DLP uses Google's leading optical character recognition to increase detection coverage and quality. DLP can also be used to prevent users from sharing sensitive content in Google Drive or shared drive with people outside of your organization.



❤️ 12 ✌️ 24

Vendor Access Control

We've designed our systems to limit the number of employees that have access to customer data and to actively monitor the activities of those employees. Google employees are only granted a limited set of default permissions to access company resources. Access to internal support tools is controlled via access control lists (ACLs).

Google follows a formal process to grant or revoke employee access to Google resources, and access is automatically removed for departing employees. Access authorization is enforced at all relevant layers of the system. Approvals are managed by workflow tools and logged. An employee's authorization settings are used to control access to all resources, including data and systems for Workspace products.

Access is monitored by our dedicated security teams as a check on the effectiveness of our controls. The security teams proactively monitor access patterns and investigate unusual events.

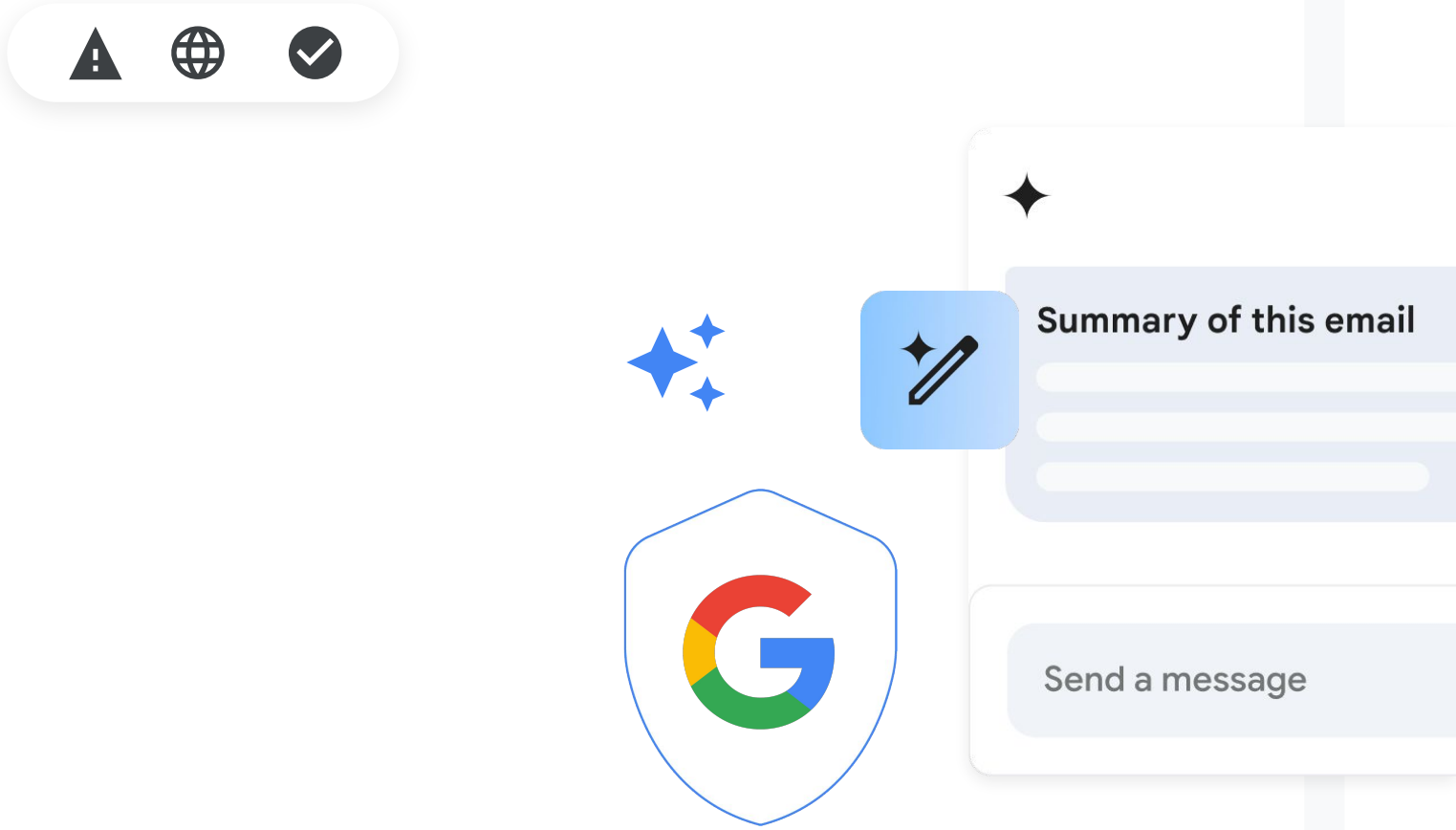
Fine-grained approvals for support

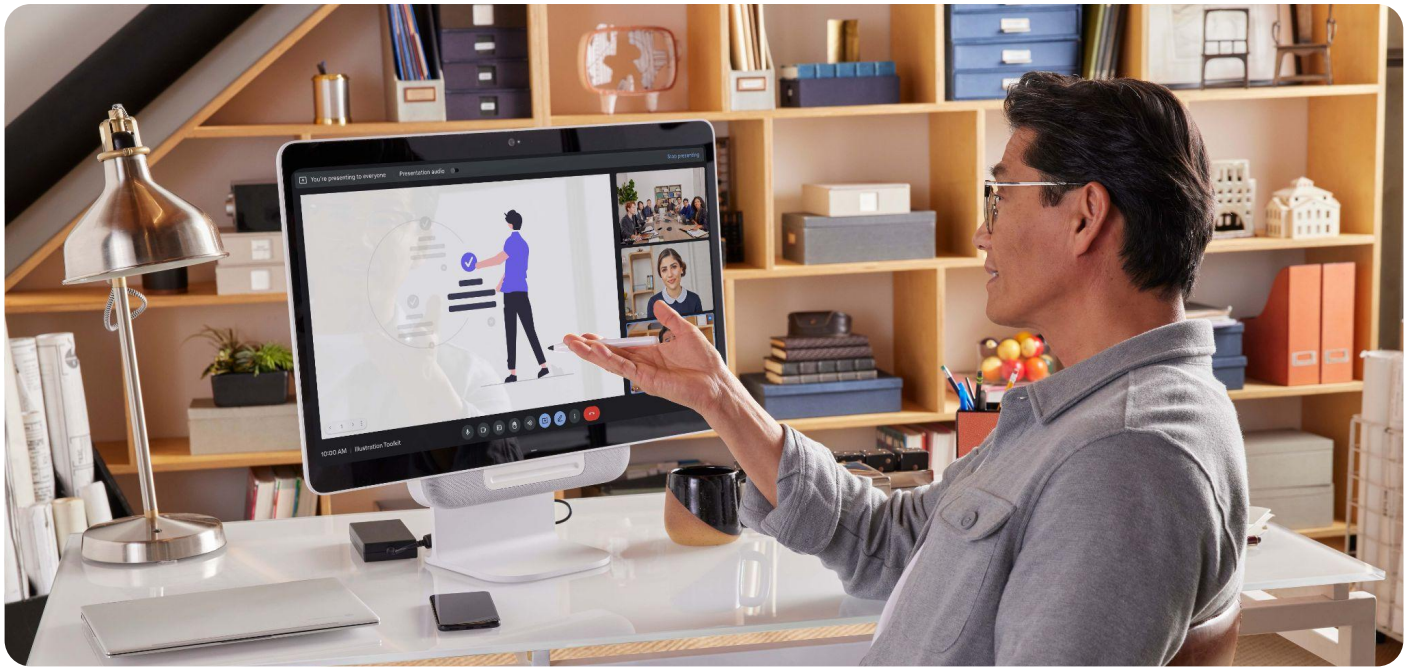
Additionally, for organizations who require data regionalization within the US to meet FedRAMP requirements, access controls within Workspace enable customers to limit the region from which Google employees access customer data for support purposes, and enforce customizable rules that require Google support staff to seek fine-grained approvals before any access to data is performed.

With Access Controls in Workspace (Access Transparency, Access Management, and Access Approvals) - you are the ultimate arbiter to your data. Customers provide explicit permission for their data to be accessed, and can request region-based support.

Furthermore, as part of Google's long-term commitment to transparency and user trust and to align with AU.L2-3.3.1, we provide Access Transparency Reports. This is a feature that enables customers to review logs of actions taken by Google staff when accessing your specific customer data. For services integrated with Access Transparency, Google uses a tool to validate that the business justification presented for access is valid, and log the justification to Access Transparency Logs.

Enhanced Cybersecurity





❤️ 12 ✌️ 24

Multi-Factor Authentication and Security Keys

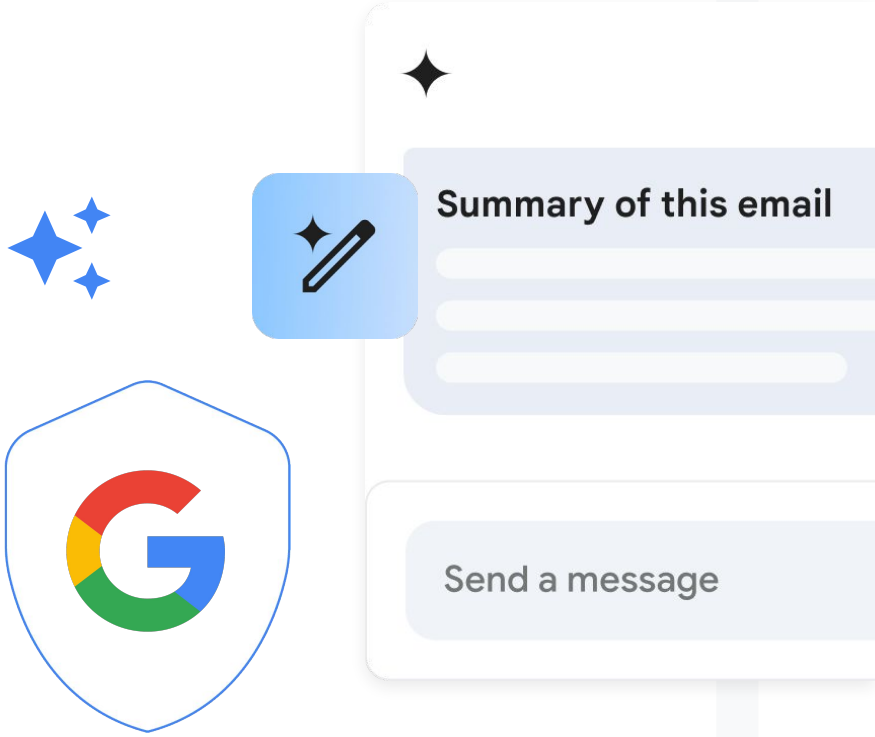
Workspace's multi-factor authentication, which aligns with CMMC IA.L2-3.5.3 helps protect against unauthorized access to CUI.

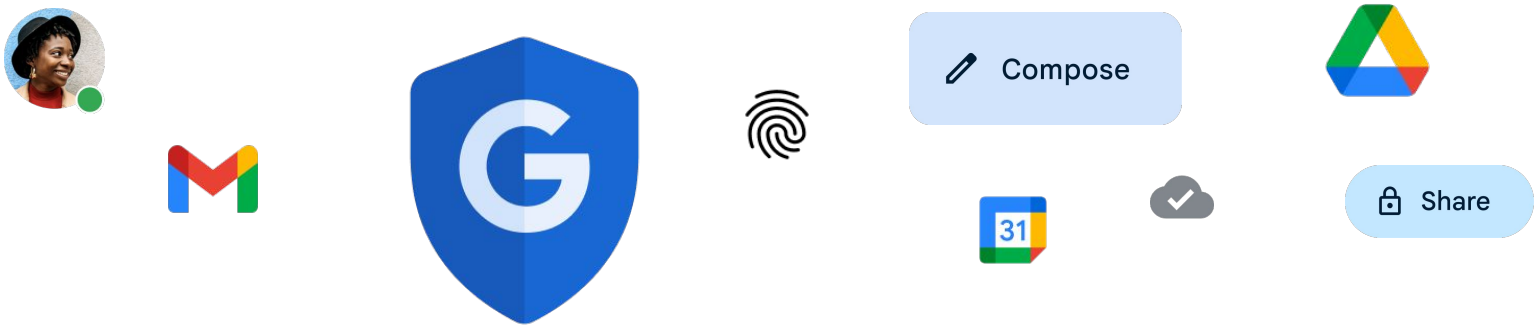
Customers can strengthen account security by using 2-step verification and security keys. These can help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts. With the Advanced Protection Program, we can enforce a curated set of strong account security policies for enrolled users. These include requiring security keys, blocking access to untrusted apps, and enhanced scanning for email threats.

Passkeys

Further combating user credential compromise, passkeys are a passwordless sign-in method that can offer a convenient and secure authentication experience across websites and apps, allowing users to sign in with a fingerprint, face recognition, or other screen-lock mechanism across phones, laptops, or desktops.

Proven Compliance **Credentials**





Certifications and audits

Workspace supports customers across a number of highly regulated industries, including government organizations. Google Cloud provides products and services in a way that enables our customers to be compliant with numerous industry-specific requirements. More information on how we meet and maintain compliance is available here.

Independent attestations

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

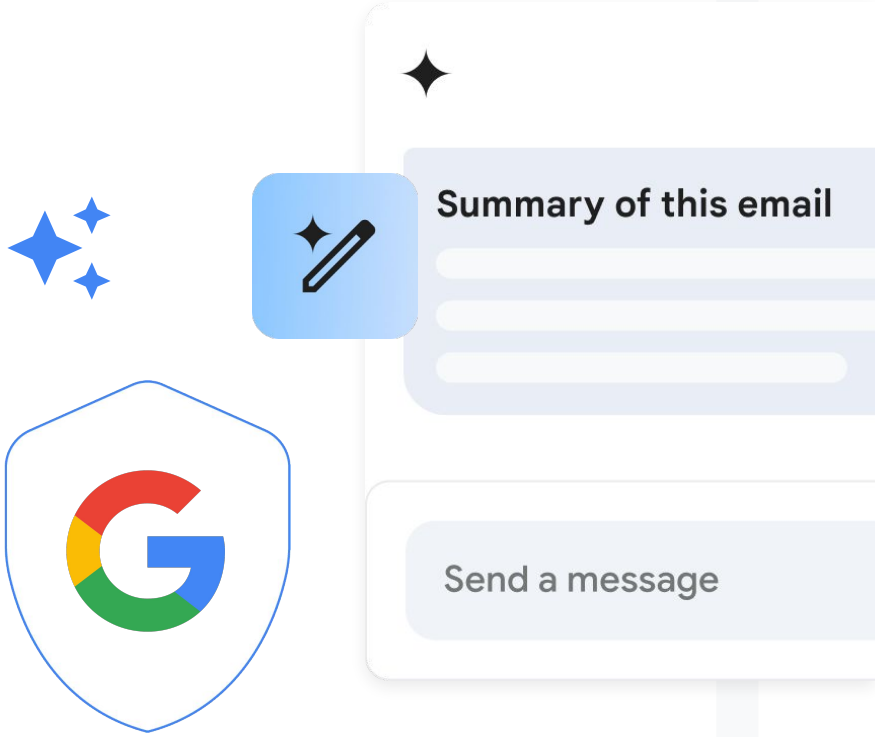
- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- ISO/IEC 27701 (Privacy)
- SOC 1, SOC 2 and SOC 3 reports

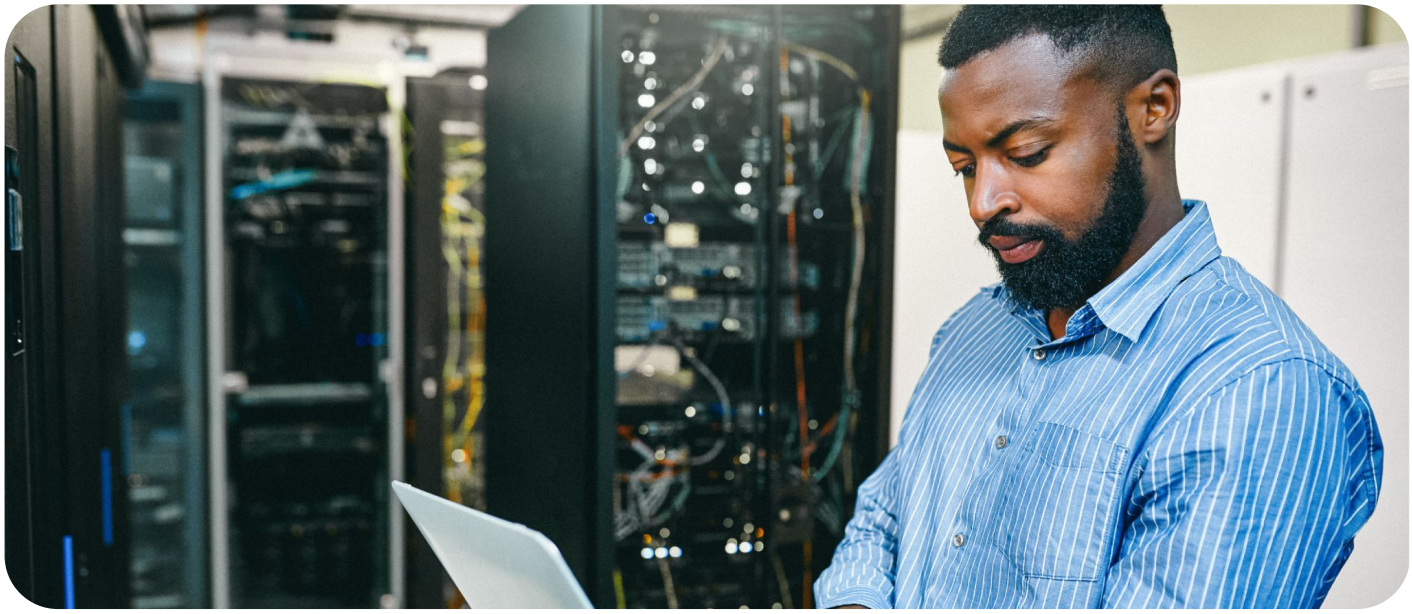
Google also participates in US public sector frameworks, such as FedRAMP (US government), ITAR, IRS 10755, CJIS, DFARS and others. Workspace services are FedRAMP High and IL4 authorized. In support of customers' CMMC compliance, Google has obtained a 3PAO attestation that Workspace supports compliance with NIST's Special Publication 800-171, the underlying controls of CMMC, when paired with customers' implementation of Google's Customer Responsibility Matrix (CRM).

We can provide resource documents and mappings to help customers meet their CMMC compliance needs such as an Implementation Guide and CRM, upon request.

We also provide resource documents and mappings for additional frameworks where formal certifications or attestations may not be required or applied to help organizations proactively address evolving regulations.

Scalable Solutions





Government-grade commercial cloud

Organizations Seeking Certification can benefit from utilizing a cloud environment with simple set up to prevent the high cost and complexity of employing third-party integrators to meet CMMC compliance.

Built-for-purpose infrastructure:

Google delivers one cloud instance for all customers, ensuring that all customers receive the same benefits, security, capacity, and feature updates at the same pace. Therefore, government and DIB customers can leverage Workspace with the assurance that the infrastructure has been built for purpose.

Streamlined cost model:

Moreover, government and DIB customers will not be subjected to the high costs of advanced security and compliance premiums running on designated government cloud environments, nor will they experience the significant delays in availability of security, compliance, and productivity features to this infrastructure.

.

Workspace leverages the same highly-reliable and secure infrastructure that powers Google's services like Search and YouTube, used by billions of people around the world daily. This foundation of global data centers with built-in redundancy ensures high availability for your workloads. Agencies can confidently host critical workloads and sensitive data, knowing that Google's infrastructure is designed for uptime and security.

Establishing a **security-first culture** with Workspace as a foundation

Achieving CMMC 2.0 compliance is an ongoing process that requires vigilance, the right tools and a security first mindset. Technology is important for compliance, but achieving CMMC 2.0 needs a broader approach of encouraging a security-first culture within your organization to scale the following:

Technology

Workspace provides a scalable, secure, and compliance-focused foundation for you to build the best practices, security policies, management and monitoring that's right for your organization, so that you can meet DoD standards and thrive in the public sector.

❤️ 12 ✌️ 24

How Workspace can help

We continue to be focused on helping organizations keep pace with evolving regulations and setting you up for success with your adherence to CMMC 2.0. Google Workspace offers public sector organizations comprehensive support for migration including possible subsidies for migration costs, dedicated assistance, specialized tools, and a network of expert partners.

To speak with our specialist team about how Workspace can support your CMMC journey, please contact us at workspacecmmc@google.com.