HITRUST®

How Organizations Can Leverage HITRUST for CMMC Compliance

Let us help you prepare for your CMMC Assessment.

What is the Cybersecurity Maturity Model Certification (CMMC)?
To address national security concerns within their third-party ecosystem, the United States Department of Defense (DoD) has mandated that all organizations doing business with the DoD—regardless of size, industry, or involvement—have the maturity of their cybersecurity operations independently certified against the newly established Cybersecurity Maturity Model Certification (CMMC) framework. Governed by an overarching Accreditation Body, the CMMC program requires every contractor to be audited by an independent third-party auditor, or Certified Third-Party Assessor Organization (C3PAO). Up until now, contractors have struggled to secure their expanded supply chains with inconsistent cybersecurity practices.

Organizations that believe they may soon be subject to these requirements should take the following steps:

1. Familiarize yourself with the HITRUST CSF® and the CMMC Model.
2. Determine what CMMC Maturity Level your organization must certify.
3. Utilizing MyCSF®: Document compliance and evaluate your current security posture against the requirements of that level.
4. Develop and execute corrective action plans (CAPs) where necessary.
5. Engage an independent third-party auditor or C3PAO.

HITRUST has a solution to help with every step of the process. When it is time for your organization to engage with an assessor, consider a C3PAO that is also a HITRUST Authorized External Assessor. This can help streamline the process by enabling simultaneous completion of both the CMMC Assessment and a HITRUST CSF Assessment.

HITRUST is here to help your organization understand and meet CMMC compliance requirements.
HITRUST's comprehensive and integrated suite of compliance and risk management solutions align with the requirements of CMMC and fully support organizations in preparing to achieve CMMC.

While the CMMC Accreditation Body (CMMC-AB) continues its efforts to bring the CMMC program to market, HITRUST customers can rest easy knowing that for every component of the CMMC program, there is a direct HITRUST program or offering that currently achieves the same objectives. The components of the HITRUST Approach™ most directly related to addressing CMMC are the HITRUST CSF, HITRUST CSF® Assurance Program, HITRUST MyCSF, and the HITRUST Assessment XChange.

The HITRUST CSF
The HITRUST CSF already integrates with and contains mappings to the same baseline standards upon which the CMMC framework is based (e.g. NIST SP 800-53 r4, NIST SP 800-171 r2*, NIST CSF v1.1, FedRAMP, and CIS Controls v7.1) and integrates the recently released CMMC framework into the HITRUST CSF version 9.4.

The HITRUST CSF Assurance Program
The HITRUST CSF Assurance Program enables organizations to assess their current security and privacy posture against these standards and achieve and maintain CMMC compliance by leveraging the many benefits of the HITRUST CSF Assurance Methodology, including Assess Once, Report Many™.

**CMMC maps to NIST SP 800-171 r1. HITRUST CSF v9.4 maps to NIST SP 800-171 r2.*

Updated 6/19/2020

HITRUST MyCSF

The MyCSF platform can be leveraged to lend insight into gaps and remediations needed to be implemented prior to performing a CMMC Assessment. MyCSF supports "what if" planning and utilizes previously entered information to streamline and simplify the process of performing a GAP analysis against the CMMC framework requirements.

Organizations that invest in a controls assessment and repository platform will be better positioned to succeed in their CMMC efforts. As is the case with many other authoritative sources to which HITRUST maps, MyCSF allows organizations to assess their posture against the requirements of CMMC in two ways. Organizations with a valid HITRUST CSF Certification should be able to determine the additional control requirements by leveraging MyCSF and performing an assessment specific to the delta in scope and requirements. Alternatively, organizations primarily interested in compliance and seeking to narrow their assessment solely to the requirements of CMMC can do a HITRUST CSF Targeted Assessment. It is critical that entities have the ability to leverage existing investments made in information risk management and compliance programs, including assurance reports developed using a comprehensive methodology, in support of CMMC.

Whether an organization chooses to assess their posture using a HITRUST CSF Targeted Assessment or full HITRUST CSF Validated Assessment with Certification, the Scorecard feature of MyCSF helps determine an organization's level of readiness, enables quick interpretation of assessment results, and—as applicable—supports remediation planning efforts.

The HITRUST Assessment XChange

Lastly, third-party assurance is another critical area subject to CMMC requirements. Organizations should not wait to begin the conversation with their third parties that have access to the DoD's sensitive information via their own systems. In all such cases, organizations must evaluate their third parties' risk and compliance posture and obtain assurances that they too can meet the same CMMC controls required of them by the DoD. The HITRUST Assessment XChange can help organizations streamline and simplify their third-party risk management, ensuring that everyone is doing their part to protect sensitive data and protecting parent organizations' interests with regards to doing business with the DoD.

> The CMMC is an effort by the DoD to ensure that their sensitive information is secure throughout the third-party ecosystem. All organizations that have access to any DoD data, whether they be prime or subprime contractors, will need to demonstrate CMMC compliance. Learn more **here**.

As the DoD and CMMC-AB move forward with developing and implementing the requirements of the CMMC, HITRUST will be at the forefront, continuing to participate as a subject matter expert and thought leader while helping simplify the road to CMMC for organizations of all sizes, across all industries.

Since our inception, HITRUST has focused on ensuring that our products and services are purposefully designed to support new market requirements. Helping new and existing customers continue to demonstrate to and obtain necessary assurances from customers and third parties is our mission and the CMMC requirements are just the latest example of how HITRUST helps organizations ***Assess Once, Report Many***. More information on the HITRUST suite of services can be found here.

Ask us about the HITRUST CMMC Scorecard™

For more information on CMMC, visit our webpage, or contact sales@hitrustalliance.net to learn how to get started on your journey to CMMC compliance.