HITRUST

How HITRUST Enables and Supports the Cybersecurity Maturity Model Certification (CMMC)

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 level of 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 aims to enforce the Defense Federal Acquisition Regulation Supplement (DFARS) and National Institute of Standards and Technology (NIST) frameworks by requiring every contractor to be audited by an independent third-party auditor or CMMC Third-Party Assessment Organization (C3PAO). Up until now, contractors have struggled to secure their expanded supply chains with inconsistent cybersecurity practices.

How has HITRUST been involved?

HITRUST® has been actively involved with the DoD and in related industry efforts to finalize the CMMC standard and the associated CMMC Accreditation Body (AB). Leveraging our 12 years of experience as a leader in delivering the highest quality assurance reports, developing our framework, assurance program, academy, assessor network, assessment infrastructure and related programs, HITRUST has made and continues to make valuable contributions and share key insights on how best to go about accrediting auditors, delivering training, and issuing certifications.

How can HITRUST help you achieve CMMC?

For many months now, HITRUST has been working to ensure that our 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 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 contemplated by the DoD, there is a direct HITRUST analog 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, and HITRUST MyCSF®. Although a final version of the CMMC framework has yet to be released, the HITRUST CSF currently integrates with and contains mappings to the same baseline standards upon which the CMMC framework is based (i.e., NIST SP 80-53, DFARS/NIST SP 800-171, and FedRAMP).

The HITRUST CSF Assurance Program enables organizations to assess their current security and privacy posture against these standards and once a final CMMC framework is released, will enable organizations to achieve and maintain CMMC, leveraging the many benefits of the HITRUST CSF Assurance Methodology, including ***Assess Once, Report Many™***.

>>>

How can HITRUST help you achieve CMMC *Continued*

The MyCSF tool can be leveraged to lend insight into GAPS and remediations needed to be implemented prior to the CMMC. 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.

MyCSF is a best in class, purposefully designed and engineered SaaS solution for performing risk assessments and corrective action plan management, including enhanced benchmarking and dashboards as well as integration with major GRC platforms and the HITRUST Assessment XChange™.

In communications from DoD, it is clear that organizations who invest in a controls assessment and repository platform will be better positioned to succeed in their CMMC efforts. 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. It is critical that entities have the ability to leverage existing investments made in information risk management and compliance programs including existing assurance reports, developed using a comprehensive methodology, in support of CMMC.

Lastly, third-party assurance is another critical area subject to CMMC requirements. Hereto, organizations cannot afford to wait to begin conversations with all third-party vendors to whom they afford access to sensitive information belonging to the DoD. 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 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.

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.

Ask us about the HITRUST CMMC Scorecard™

About HITRUST

Since its inception, HITRUST has made a focus of ensuring that its products and services – namely the HITRUST CSF framework, HITRUST MyCSF, HITRUST CSF Assurance Program, and HITRUST Assessment XChange – 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 is just the latest example of how HITRUST helps organizations ***Assess Once, Report Many***™. More information on the HITRUST suite of services can be found at **https://hitrustalliance.net/the-hitrust-approach/.**