With the initial inclusion of CMMC requirements slated to appear in Department of Defense RFIs and RFPs (requests for information/proposals) in late 2020/early 2021, many contractors may still be uncertain where to begin. We’ve got you covered.

Use our high-level road map to help get you started on your journey toward compliance.

1. Review the CMMC framework to understand the practices and processes your organization would need to comply with for the level of maturity desired.
2. Conduct a preparedness assessment – work with a third party or with your team to identify technical gaps in existing vs. required practices.
3. Develop and implement practices that are found to be non-existent (or fixes for those determined weak) based on the results of the assessment.
4. Deploy technical solutions where needed.
5. Remediate other process gaps as identified in the preparedness assessment.
6. Identify/select a CMMC Third-Party Assessor Organization (C3PAO) firm for your CMMC audit.
7. Obtain your desired CMMC level maturity certification based on the audit.
8. Obtain your desired CMMC level maturity certification based on the audit.

CONTACT
Bhavesh Vadhani, Principal
National Director, Cybersecurity, Technology Risk, and Privacy
703.847.4418 | bhavesh.vadhani@cohnreznick.com

CohnReznick LLP © 2020 | This has been prepared for information purposes and general guidance only and does not constitute legal or professional advice. You should not act upon the information contained in this publication without obtaining specific professional advice. No representation or warranty (express or implied) is made as to the accuracy or completeness of the information contained in this publication, and CohnReznick LLP, its members, employees and agents accept no liability, and disclaim all responsibility, for the consequences of you or anyone else acting, or refraining to act, in reliance on the information contained in this publication or for any decision based on it.