Why was it created?

The intent of **the Cybersecurity Maturity Model Certification (CMMC) is to ensure that** organizations working with the DoD have security measures in place in order to reduce unauthorized exfiltration of Federal Contract Information (FCI) and Controlled Unclassified Information (CUI).

How does CMMC affect my organization?

Firstly, your organization will be required to meet a particular CMMC level to apply for DoD projects.

Secondly, this framework is designed to assist the organization to enable security on all levels and therefore reduce the risk to the organization.

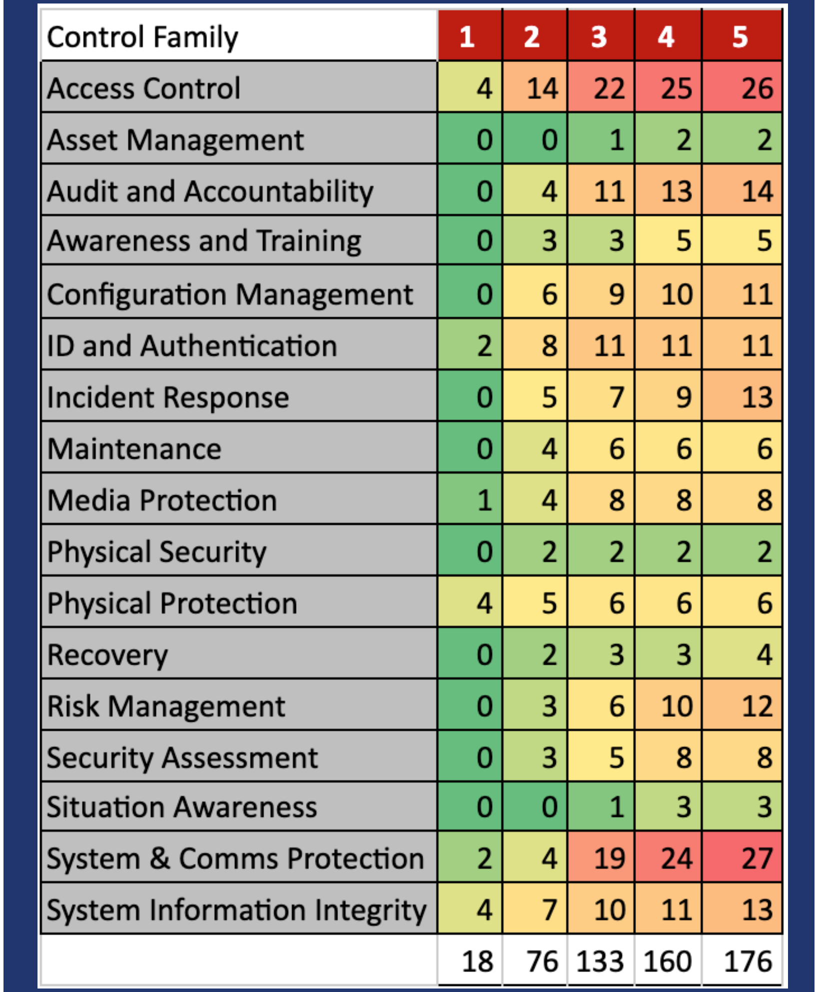
How does Corvid Cyberdefense assist in achieving CMMC compliance?

We work with your organization to deploy our Haven security tools and 24/7 monitoring by our US-based security operations center to help you achieve many of the CMMC requirements. A detailed description of how Haven delivers CMMC requirements and compliance documentation templates can be provided.

We also offer vCISO (virtual chief information security officer) services for organizations that would like guidance or a dedicated advisor to walk through each step of the compliance process.

Contact us today to find out how we can help you achieve CMMC compliance.

5 Levels of CMMC



Control Family	1	2	3	4	5
Access Control	4	14	22	25	26
Asset Management	0	0	1	2	2
Audit and Accountability	0	4	11	13	14
Awareness and Training	0	3	3	5	5
Configuration Management	0	6	9	10	11
ID and Authentication	2	8	11	11	11
Incident Response	0	5	7	9	13
Maintenance	0	4	6	6	6
Media Protection	1	4	8	8	8
Physical Security	0	2	2	2	2
Physical Protection	4	5	6	6	6
Recovery	0	2	3	3	4
Risk Management	0	3	6	10	12
Security Assessment	0	3	5	8	8
Situation Awareness	0	0	1	3	3
System & Comms Protection	2	4	19	24	27
System Information Integrity	4	7	10	11	13
	18	76	133	160	176

Number of Control Family requirements to achieve each level of CMMC

PLAN. PROTECT. PRE-EMPT

cyvent.com | yuda@cyvent.com | +1 (305) 299-1188