CMMC AND CLOUD COMPLIANCE

- The Cybersecurity Maturity Model Certification (CMMC) is a standard for measuring cybersecurity effectiveness.
- Developed by the Department of Defense, CMMC measures and rates the cybersecurity practices of organizations supplying services to the DoD

- CMMC is based on NIST CSF and NIST SP 800-171
- These frameworks are used across all industries to help companies gauge their cybersecurity effectiveness
- CMMC can help companies that want a method for achieving higher levels of security

171 Practices

5 Processes

17 Capability Domains

Access Control (AC)	Asset Management (AM)	Awareness & Training (AT)	Audit & Accountability (AN)	Configuration Management (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)
Personal Security (PS)	Physical Protection (PE)	Recovery (RE)	Risk Management (RM)	Security Assessment (CA)	Situational Awareness (SA)	System & Communications Protection (SE)	System & Information Integrity (SI)	

All the major cloud providers have a shared responsibility approach to helping their customers achieve NIST 800-171 and CMMC compliance. Cloud Providers take care of the physical operations of their cloud and Cloud Customers take care of the data and applications in their “instance”.

SHARED RESPONSIBILITY APPROACH

MONTRA

1425 Ellsworth Industrial Blvd NW
Suite 18, Atlanta, GA 30318
(404) 665-9675
montra.io