THE 17 CMMC CYBERSECURITY CAPABILITY DOMAINS

Access Control (AC)
- Establish system access requirements
- Control internal system access
- Control remote system access
- Limit data access to authorized users and processes

Asset Management (AM)
- Identify and document assets
- Manage asset inventory

Audit and Accountability (AU)
- Define audit requirements
- Perform auditing
- Identify and protect audit information
- Review and manage audit logs

Awareness and Training (AT)
- Conduct security awareness activities
- Conduct training
- Identify and protect audit information

Configuration Management (CM)
- Establish configuration baselines
- Perform configuration and change management

Identification and Authentication (IA)
- Grant access to authenticated entities

Incident Response (IR)
- Plan incident response
- Detect and report events
- Develop and implement a response to a declared incident
- Perform post-incident reviews
- Test incident response

Maintenance (MA)
- Manage maintenance

Media Protection (MP)
- Identify and require media
- Protect and control media
- Sanitize media
- Protect media during transport

Personnel Security (PS)
- Screen personnel
- Limit physical access
- Protect controlled unclassified information (CUI) during personnel actions

Physical Protection (PE)
- Manage security
- Manage information security continuity

Recovery (RE)
- Manage backups
- Manage supply chain risk

Risk Management (RM)
- Identify and evaluate risk
- Manage risk

Security Assessment (CA)
- Develop and manage a system security plan
- Define and manage controls
- Perform code reviews

Situation Awareness (SA)
- Implement threat monitoring
- Control communications at system boundaries

System and Information Integrity (SI)
- Define security requirements for systems and communications

System and Communications Protection (SC)
- Identify and manage information system flaws

Common industry framework references
- NIST 800-171
- NIST CSF
- ISO 27001