CMMC Compliance Checklist: 17 Domains

How To Comply & How We Can Help

ACCESS CONTROL

How to Comply: Establish who has access to your systems, control internal system access, and limit data access to authorized users and processes.

How We Help: We will establish and maintain a domain structure which uniquely identifies users, enforces security and CUI policies, and controls local and remote access. We handle the IT onboarding and offboarding of employees and grant and revoke access to your information and systems, whether on-premises or in the cloud.

ASSET MANAGEMENT

How to Comply: Locate, identify and log inventory of all your company assets.

How We Help: Our automated tools constantly poll your internet connected computers. Hardware and softwa re inventories are provided on your schedule. We also track warranty and license expirations.

AUDIT & ACCOUNTABILITY

How to Comply: Have a process in place to track users that have access to your CUI and perform secure audits of those logs to ensure accountability.

How We Help: We will define your audit requirements, perform the audit, identify and protect your audit information, as well as review and manage your audit logs. We will maintain audited events for as long as you subscribe to the service.

AWARENESS & TRAINING

How to Comply: Put security awareness training programs in place for all employees.

How We Help: We provide monthly phishing prevention training and regular employee security awareness activities.

CONFIGURATION MANAGEMENT

How to Comply: Establish configuration baselines as a measure to judge the efficiency of your systems.

How We Help: We will establish your baseline configuration and perform configuration and change management tasks on an ongoing basis.

IDENTIFICATION & AUTHENTICATION

How to Comply: Ensure the proper roles within your organization have the correct level of access and can be authenticated for reporting and accountability purposes.

How We Help: We can ensure only users authorized by you have the credentials to access data and systems. We also handle all aspects of user account creation and maintenance.

INCIDENT RESPONSE

How to Comply: Establish an incident response plan that detects and reports events, implement responses to a declared incident, post-incident reviews and test responses to measure your preparedness in the event of an attack.

How We Help: We will create an incident response plan, test the incident response plan, detect and report ongoing events, develop responses to declared incidents and perform post incident reviews.

MAINTENANCE

How to Comply: Have a maintenance system in place to effectively operate your systems.

How We Help: System patches will be pushed on recurring weekly and monthly schedules. Zero-day vulnerabilities will be pushed within 24 hours.

MEDIA PROTECTION

How to Comply: Provide proof that your media is identified and marked for ease of access. Additionally, provide evidence that a media protection protocol, sanitation protocol and transportation protection is in place.

How We Help: We can help identify and mark all media, put process in place to protect and control media, and sanitize and protect media for transport.

PERSONNAL SECURITY

How to Comply: Ensure all personnel will be properly screened and have background checks completed. Provide evidence that CUI is protected during personnel activity such as employee turnover or transfer.

How We Help: We provide customized onboarding and offboarding checklists to ensure your business process is reflected in user account management. Only designated client POCs can request changes to access.

PHYSICAL PROTECTION

How to Comply: Provide evidence of the physical security surrounding your assets and prove they are protected.

How We Help: While mainly a client activity, we can assist with system maintenance, vendor coordination, and best practice consulting.

RECOVERY

How to Comply: Keep and log backups of media necessary to your organization, and log for the purpose of continuity and to mitigate lost data.

How We Help: We can automate backups on the schedule that meets your needs, by either adapting your existing systems to comply with CMMC or implementing a new, compliant system.

RISK MANAGEMENT

How to Comply: Identify and evaluate the risk that affects your company using periodic risk assessments and vulnerability scanning - both yours and your vendors.

How We Help: We can create Risk Management Plans and offer custom consulting for specific risk mitigations strategies and actions.

SECURITY ASSESSMENT

How to Comply: Put a system security plan (SSP) in place, define and manage controls and perform code reviews.

How We Help: We can create or update your SSP/POAM as part of a CMMC Readiness Assessment, during a discovery phase and/or as part of your on-boarding to Ntiva services.

SITUATIONAL AWARENESS

How to Comply: Establish a threat monitoring system to help keep your organization secure in event of cyber incidents.

How We Help: Managed EDR and IDR with our 24/7 SIEM/SOC solution allows for rapid detection and mitigation of threats to your environment.

SYSTEM & COMMUNICATIONS PROTECTION

How to Comply: Define the security requirements of each system and communication channel you use to provide evidence that you have control of communications at system boundaries.

How We Help: We help define your requirements and then implement the tools, technologies, and processes to protect your systems whether on-prem or in the cloud - especially important in today's remote workforce.

SYSTEM & INFORMATION INTEGRITY

How to Comply: Identify and manage flaws with your system, identify hazardous and malicious content in-system, implement email protections and monitor your network and systems.

How We Help: Vulnerability scans and remediation, EDR, IDR and cloud-based email protections block malicious content, monitor your network, and alert our 24/7 SOC and Service Desk of any suspicious behavior.