ATS' NIST 800-171 and CMMC Engagement Approach

ATS will provides consulting services to our government contractor clients with the purpose of assisting these companies in reaching the necessary level of compliance to satisfy government regulations and standards to perform NIST 800-171 self-assessment and prepare for CMMC compliance.

ATS' approach entails three main phases, where our client management team works closely with the client POC(s) to pull in all the necessary resources that will help the client implement the necessary improvements to comply and meet the NIST 800-171 self-assessment and prepare for the upcoming CMMC audits. The different phases are described below:

Phase 1: Gap Assessment and Documentation Creation

This phase is performed by ATS' partner OCD Tech.

The OCD Tech team examines our clients' current policies, procedures, and their control environment for compliance against the CMMC requirements for the target level (L1 to L5). The output from this phase is a System Security Plan (SSP) and a Plan of Action & Milestones (POAM).

This phase typically takes three weeks to complete, depending on the maturity of the organization's current policies and security posture.

Phase 2: Remediation

Performed by the ATS client management and technical teams with support from OCD Tech.

At the conclusion of Phase 1, we provide the client with a bundle of documentation, including the Plan of Action & Milestones. This document, part of the requirements of DFARS, is a list of security requirements that are partially or not implemented in the client's environment. ATS reviews the list with the client, providing our cost-conscious recommendations as to how the ATS team will configure and help implement these controls.

As part of the remediation, ATS will typically move client applications to Azure for Government. ATS assists with the analysis, planning, and budgeting to perform such a migration. Solutions would utilize the security and compliance monitoring features of Azure for Government. ATS can then manage and monitor the client systems in Azure for Government.

If necessary, ATS usually recommends that the client migrates to Microsoft 365 GCC or GCC High and configure security features and controls in the Microsoft 365 environment to meet NIST 800-171 and CMMC requirement needs.

Migrating on-prem file and SharePoint server content to SharePoint Online is also a popular decision with our clients to place more stringent controls over their content.

The length of time that this phase takes is dependent on the resources working the remediation and the client availability for the work to proceed.

Phase 3: Documentation Finalization

Once ATS and client have remediated all or most of the items in the Plan of Action & Milestones, OCD Tech's team will review and verify the work performed and finalize the bundle of documentation we initially created in Phase 1.

These documents represent the evidence required to verify DFARS compliance with the client's prime, DoD, or DCMA customer. The output from this phase includes finalized documentation, as well as a point-in-time self-assessment score, which will also prepare the client for the upcoming CMMC audits.

This phase typically takes one week to complete.