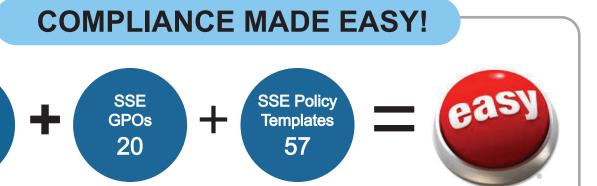


NIST 800-171 & CMMC SOLUTIONS



STEP 1:

SSE

Tech Stack

Plan - Readiness Assessment

- Assess current environment and future needs
- Determine level of CMMC compliance needed
- Summary review of existing SSP and POAMs (if possible)
- Develop roadmap for CMMC compliance
- Define high-level budget

STEP 3:

Protect - Remediation

- Document Policies/Procedures SSE Model **Policy Templates**
- Customized client specific administrative policies and practices
- SSE Tech Stack/GPO specific IT policies and practices
- Implement IT Plan SSE Tech Stack + GPOs
- Server/Workstation Configurations
- Hardware/Software Installations
- Finalize System Security Plan (SSP)

STEP 2:

Prepare - Gap Analysis

- Review Existing Policies/Procedures
- Review IT Environment
- Review Physical Security Practices
- **Audit Entirety of Evidence Collected**
- Identify/Document Gaps
- Provide Security Assessment Report (SAR) and POAMs

STEP 4:

Perform – Steady State Operations

- Cybersecurity As A Service
- On-going outsourced management of SSE Tech Stack and GPOs
- Continuous monitoring/remediation of issues
- Continuous audit/evidence collection to demonstrate compliance to policies
- Internal Self-Assessment (at least annually)