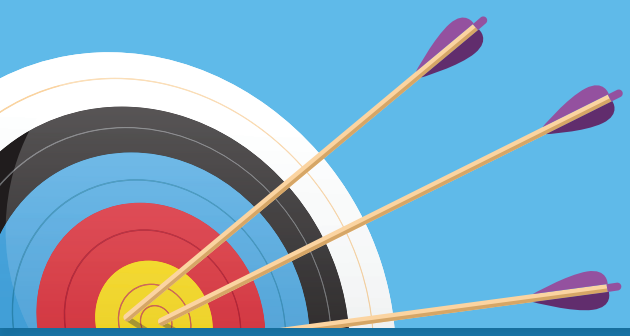

DFARS Engagement Approach

Our DFARS engagement approach is composed of three phases spanning the length of the project.

WORK AREAS:

PHASE 1: GAP ASSESSMENT AND DOCUMENTATION CREATION

Performed by: OCD Tech
We examine your current policy, procedure, and control environment for compliance against the DFARS requirements. The output from this phase is a current-state System Security Plan, Plan of Action & Milestones, Cyber Incident Reporting Process, Acceptable Use Policy, and Controlled Unclassified Policy

Time to complete: Typically two weeks

PHASE 2: REMEDIATION

Phase 2: Remediation
Performed by: Company, with recommendations and support from OCD Tech
At the conclusion of Phase 1, we provide you 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 your environment. We provide this list along with cost-conscious recommendations as to how to implement these controls.

Time to complete: Dependent on company resources

PHASE 3: DOCUMENTATION FINALIZATION

Once you have remediated all or most of the items in your Plan of Action & Milestones, we review and verify the work you have performed and finalize the bundle of documentation we initially created in Phase 1. These documents represent the evidence required to verify DFARS compliance with your prime, DoD, or DCMA customer.

Time to complete: Typically one week

Important Note:
This compliance effort is not meant to be a "one and done" but rather a continuous effort. System Security Plans should be kept up-to-date at all times and reassessed annually or after major organizational or system changes.

Contact Us

Michael Hammond
CISA, CRISC, CISSP
Principal
844-OCDTECH
mhammond@ocd-tech.com

Robbie Harriman
CISA
Senior IT Audit Manager
844-OCDTECH
rharriman@ocd-tech.com