CMMC L2 ACCELERATOR

- VERIFY PRACTICES THAT MEET ASSESSMENT OBJECTIVES.
- GET A CUSTOMIZED READINESS ROADMAP TO CLOSE GAPS IN COMPLIANCE.
- STRUCTURE DOCUMENTATION FOR EASE OF REPORTING.

PROCELLIS TECHNOLOGY

ACCELERATE YOUR PATH TO CMMC LEVEL 2 COMPLIANCE

Achieving CMMC Level 2 compliance doesn't have to be daunting.

Our CMMC Accelerator is designed for Organizations Seeking Certification Assessment or compliance with the NIST SP 800-171 Rev 2 Cybersecurity Framework.

This engagement offers a streamlined and tailored approach to help your organization meet its compliance goals efficiently.

We'll identify gaps, prioritize remediation efforts, and prepare you for a successful certification assessment, ensuring you stay competitive in the Defense Industrial Base (DIB) supply chain.

DELIVERABLES

PROGRESS REPORTING

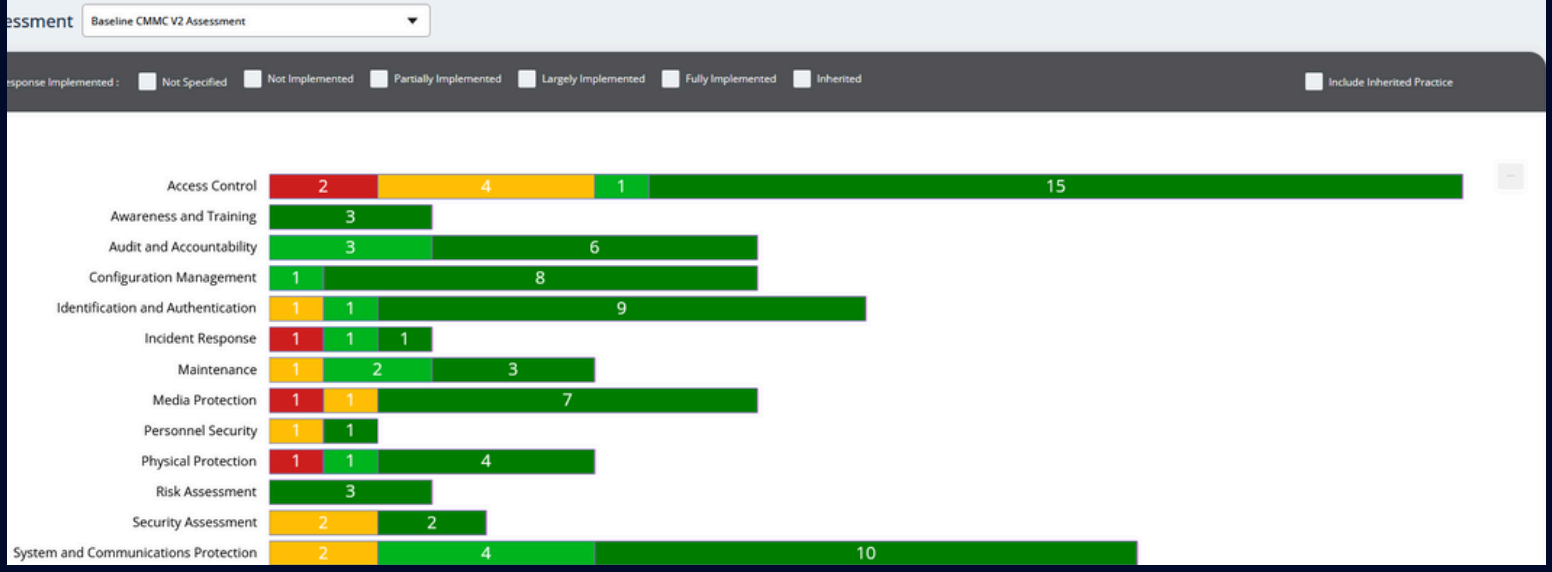
Estimated compliance score at the beginning and end of engagements with highlighted strengths and weaknesses.

PLAN OF ACTION AND MILESTONES (POAM)

This prioritized plan outlines your remediation efforts, tailored to your resources, to resolve control deficiencies.

BASELINE SYSTEM SECURITY PLAN (SSP)

Assessment ready documentation detailing how your organization fulfills control requirements to safeguard Controlled Unclassified Information (CUI).



The Engagement

This virtual engagement lasts 12 weeks and includes roughly 16 working sessions, each lasting 90 minutes. Stakeholders should expect to commit 2-3 hours per week to meetings and interim assignments.

We leverage the Cyturus compliance automation platform to systematically organize policies, procedures, and evidence, enabling real-time tracking and visibility of readiness efforts for the duration of the engagement and delivering both the PoAM and SSP.

Approach

We will assess current cybersecurity practices and guide you through identifying and remediating gaps, ensuring that all evidence and artifacts generated during the engagement meet the “sufficiency” and “adequacy” requirements for assessment objectives.

Here’s how the process unfolds:

Planning & Scoping

Assess Compliance Posture

Delivery of PoAM and SSP

Progress Report Delivery

PLANNING & SCOPING

We'll identify the stakeholders required for the engagement and define which systems, networks, and processes must be reviewed based on where Controlled Unclassified Information (CUI) is stored, processed, and transmitted in your environment.

We'll establish objectives for scoping and create a detailed project plan with defined activities, timelines, roles, and responsibilities for the engagement.

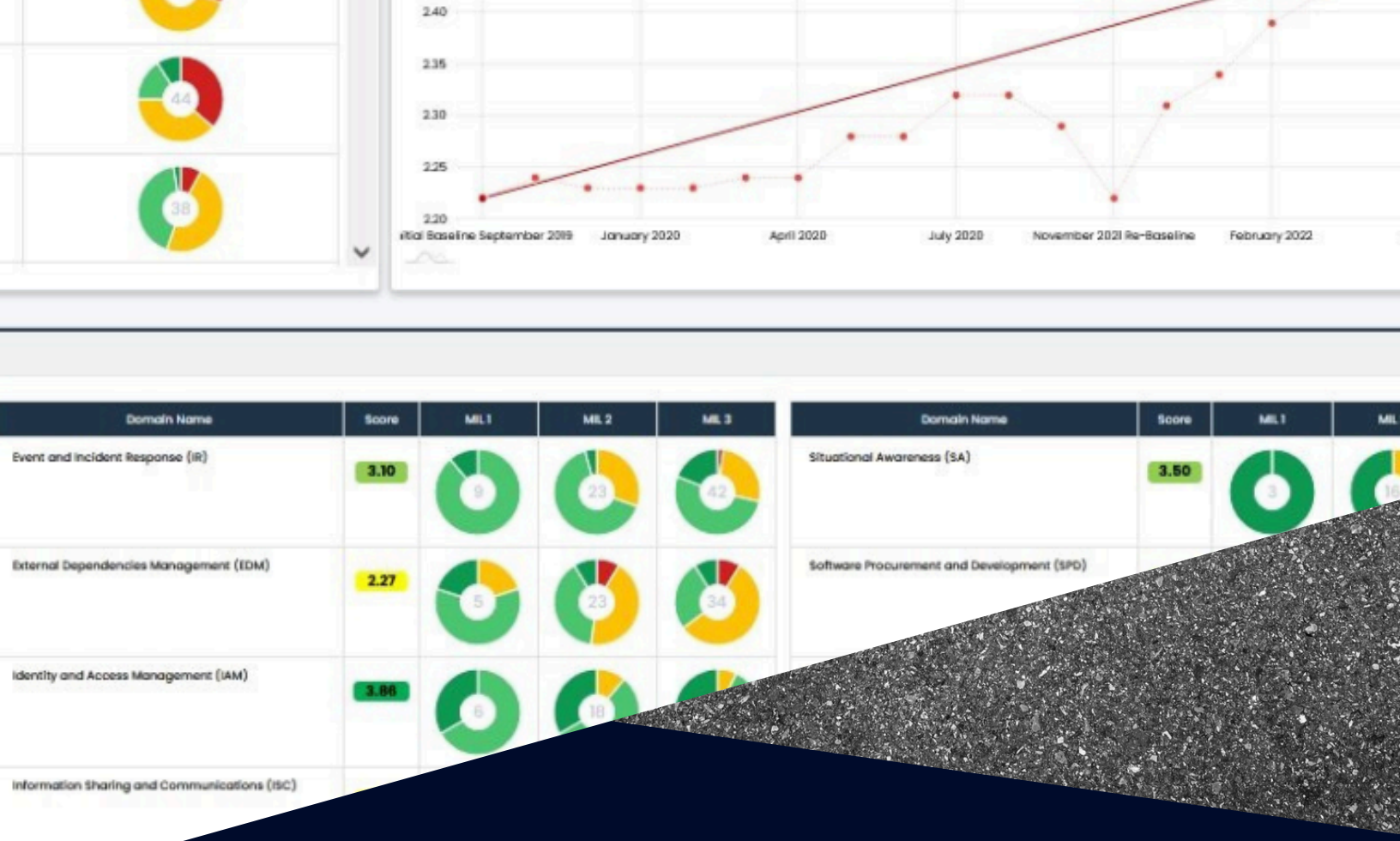
ASSESS COMPLIANCE POSTURE

Understanding your current cybersecurity posture is essential for identifying gaps for remediation and streamlined management.

We'll conduct a gap assessment to compare your current practices against the 320 assessment objectives of NIST SP 800-171A Rev 1 - The assessment criteria of the NIST SP 800-171 Rev 2 cybersecurity framework.

AREAS OF REVIEW

- Processes and procedures associated with NIST SP 800-171 Rev 2 control requirements.
- Assets, including all hardware, storage, endpoints, software, applications, and data assets within scope, with locations, versions, patch levels, and configurations.
- Network topography, including LAN, WAN, and internet connections, verifying all network segments, subnets, and critical network devices such as routers, switches, and firewalls.
- VPN Usage and secure remote access solutions.
- User access management, including provisioning, de-provisioning, and role-based access controls.
- Access encryption mechanisms for data at rest and in transit.
- Data classification, handling, and disposal procedures.
- Multifactor Authentication (MFA) implementation and password policies.
- Verify the presence of incident detection tools and Incident Response (IR) procedures.
- Endpoint protection measures, including antivirus, antimalware, endpoint detection and response (EDR) solutions, and patch management.
- Processes for managing third-party vendors and their access to CUI.
- Physical security measures to protect CUI.
- Employee cybersecurity training and awareness programs



REPORTING

We will provide an initial estimated assessment score and a final score at the end of the engagement to document the progress made. Reports will highlight areas of strength and weakness, ensuring that all stakeholders understand their compliance maturity status.

PoAM

Your plan will be customized to your timeline, environment, and resources helping you meet compliance requirements today and efficently manage them for the long haul.

SSP

We will develop an SSP that can be enriched as you advance through your PoAM. SSPs are structured for easy use by C3PAO Assessors, minimizing the risk of false starts and reducing friction during the assessment process.

WORK WITH US

Helping Organizations get CMMC compliant since 2019!

Procellis is a Cyber-AB Registered Practitioner Organization (RPO) that has successfully guided over 60 organizations to achieve CMMC compliance—and the number is still growing!

Whether starting your CMMC journey or ensuring assessment readiness, our hands-on approach provides practical guidance tailored to your current stage to advance your compliance maturity level.

All engagements are led by Certified CMMC Professionals (CCPs) and Certified CMMC Assessors (CCAs) who have years of experience in helping organizations build maturity in their compliance posture.

We don't just help you achieve compliance; we assist you in developing a streamlined compliance management program for lasting success in the DIB supply chain.

PHONE

763-219-4187

EMAIL

sales@procellis.com

WEBSITE

PROCELLIS.COM

PROCELLIS TECHNOLOGY

Minneapolis | MN

CYBER AB REGISTERED PRACTITIONER ORGANIZATION RPO

SBA U.S. Small Business Administration SERVICE-DISABLED VETERAN-OWNED CERTIFIED