

CYBERSECURITY-AS-A-SERVICE · DEFENSE INDUSTRIAL BASE

# BUILD THE PROGRAM. OPERATE THE CONTROLS.

The government can't review your intentions, but they can test your evidence **and an inflated SPRS score is a False Claims Act liability waiting to happen**. RADICL helps build your program's rationale, evidence, and documentation to be assessor-ready by working alongside your team to create the assets assessors expect. We then operate the controls to run the detection, response, and monitoring that keep them continuously performing to produce a defensible score and evidence that holds up under rigorous assessment, not just a self-attestation.

## 110

### BUILD

#### MANAGED COMPLIANCE ASSURANCE (MCA)

CMMC Level 2 requires documented, demonstrable compliance across 110 practices. The assessment is rigorous, the evidence requirements are specific, and the complexity of sustaining a compliant program is significant. MCA provides the platform, CMMC Certified Assessor (CCA) guidance, and documentation infrastructure to help build a program that will hold up under C3PAO (CMMC Third-Party Assessment Organization) assessment.

- **Platform** — Centralized control for policies, procedures, evidence, and conformity statements, giving assessors everything they need in one place.
- **Readiness** — Our team, led by a CCA, will review all controls across all 110 practices, with hands-on expert review to confirm implementation evidence, expose hidden gaps, and produce a prioritized path to assessment readiness.
- **Docs** — SSP, POA&M, and complete audit package built to CMMC Level 2 requirements, purpose-built for your environment.
- **Expert support** — Dedicated compliance team advises on what passing looks like before an assessor arrives.

Program-Wide · All 14 Domains

## 31

### OPERATE

#### MDR · MAS · MSA · MLA

RADICL CSaaS performs ongoing cybersecurity work across 31 requirements (83 assessment objectives) — running managed detection and response, vulnerability management, incident response, and security awareness directly, and extending continuous monitoring across the tools your IT team or MSP already run. You get direct coverage beyond just a policy that says a control should be working.

- **24/7 vSOC monitoring** — Continuous detection and response across endpoint, identity, and network with weekly threat hunts and custom analytics.
- **Vulnerability management** — Continuous scanning and prioritized remediation guidance, with rescans to confirm closure and flag regressions.
- **Incident response** — vSOC-led containment, case documentation, and evidence production with assessment-ready artifacts from every event.
- **Security awareness** — Annual training, phishing simulation, and custom content covering CUI handling and insider threat recognition.

31 Requirements · 83 Assessment Objectives

## KNOW EXACTLY WHO COVERS WHAT BEFORE THE AUDIT

Every RADICL engagement includes a **Shared Responsibility Matrix (SRM)**, a documented breakdown of which CMMC controls RADICL actively operates, which are shared, and which belong to your organization. No room for ambiguity, and no surprises in the assessment room.

**110** NIST 800-171  
Controls Mapped

# COVERAGE IN PRACTICE

Below are representative controls from each coverage layer, showing what RADICL does and what your program needs to demonstrate for CMMC Level 2.

## BUILD

MCA provides the platform, guidance, and documentation to address these controls. Your compliance experts help you build the program artifacts a C3PAO will ask to see.

### IA.L2-3.5.3

#### Multifactor authentication for local and network access

##### WHAT CMMC REQUIRES

Documented MFA policy, implementation evidence across all access types, and a defined exception process for privileged accounts.

##### HOW MCA ADDRESSES IT

MCA's Readiness phase includes a guided review of your Conditional Access configuration against this control's assessment objectives. Your expert flags CA policies running in report-only mode, documents which user populations are in scope, and helps produce a conformity statement tied to each objective. Policy, procedure, and evidence are managed in the Platform.

### SC.L2-3.13.1

#### Monitor, control, and protect communications at external boundaries

##### WHAT CMMC REQUIRES

Documented network architecture, boundary protection evidence, and a System Security Plan that accurately scopes what is and is not in the CUI environment.

##### HOW MCA ADDRESSES IT

MCA's Docs component works with you to produce the network architecture section of your SSP, defining the CUI enclave boundary and documenting all external communication pathways. Our team of experts confirms that the scoped environment reflects what is in and out of CUI scope and ensures the SSP satisfies assessor documentation requirements.

### CA.L2-3.12.3

#### Monitor security controls on an ongoing basis

##### WHAT CMMC REQUIRES

A defined continuous monitoring program with documented assessment frequency, assigned roles, and evidence that reviews are being conducted on schedule.

##### HOW MCA ADDRESSES IT

MCA helps define your continuous monitoring program by working with you to define assessment frequencies per control domain and identify employees with roles of responsibility.

### MP.L2-3.8.1

#### Protect system media containing CUI

##### WHAT CMMC REQUIRES

A documented media protection policy with defined handling, labeling, and disposal procedures for any media that contains or has contained CUI.

##### HOW MCA ADDRESSES IT

MCA's Readiness phase includes an expert guided assessment of what constitutes CUI-bearing media in your environment and which handling and disposal procedures are required. The Docs component works with you to produce the media protection policy and SSP section with enough specificity to satisfy assessment objectives across access, marking, sanitization, and transport.

# OPERATE

- Managed Detection & Response (MDR)
- Managed Security Awareness (MSA)
- Managed Attack Surface (MAS)
- Managed Log Analytics (MLA)

RADICL actively operates coverage for these controls, from fully-managed detection and response to continuous monitoring across the tools your IT team or MSP already run.

## SI.L2-3.14.6

### Monitor the system to detect attacks and indicators of potential attacks

#### WHAT CMMC REQUIRES

Continuous monitoring of inbound and outbound communications traffic with documented detection capability and evidence of active response to identified indicators.

#### HOW RADICL OPERATES IT

MDR across endpoints, identities, and infrastructure runs 24/7. Built-in and custom detection analytics monitor all network traffic. Each detection generates a vSOC case with full event documentation usable as assessment evidence.

## IR.L2-3.6.2

### Track, document, and report incidents

#### WHAT CMMC REQUIRES

A documented incident tracking capability with evidence that incidents are recorded, communicated to appropriate parties, and resolved with a documented timeline.

#### HOW RADICL OPERATES IT

The vSOC opens, tracks, and closes cases in the RADICL Platform. As part of MLA and MDR, every incident is tracked in a case with evidence and an audit trail, including a full event timeline, analyst notes, and closure documentation. These records are directly available as CMMC assessment evidence.

## RA.L2-3.11.2

### Scan for vulnerabilities in organizational systems periodically and when new vulnerabilities are identified

#### WHAT CMMC REQUIRES

Defined scanning frequency, evidence of scans being run on schedule, and documented remediation of identified vulnerabilities with confirmation that findings were resolved.

#### HOW RADICL OPERATES IT

MAS runs continuous vulnerability scans across enrolled assets. Prioritized findings are tracked to closure, with rescans to confirm remediation. Regression findings are flagged and escalated automatically.

## AT.L2-3.2.3

### Provide security awareness training on recognizing and reporting potential indicators of insider threat

#### WHAT CMMC REQUIRES

Documented training program with evidence that all personnel have completed insider threat awareness training including CUI handling, reporting obligations, and behavioral indicators.

#### HOW RADICL OPERATES IT

MSA delivers and tracks annual training and phishing simulation. Training content covers CUI handling, insider threat indicators, and reporting requirements. Completion records are maintained as assessment evidence.