

CMMC LEVEL 2 CONTROL COVERAGE

CMMC Level 2 consists of 110 requirements across 14 domains. RADICL's Managed Compliance Adherence (MCA) helps prepare organizations for assessment by guiding full implementation of NIST SP 800-171 Rev2. RADICL's managed security offerings provide additional compliance support, **directly addressing 31 of the most costly and difficult to implement controls to further accelerate compliance across 10 domains.**

RADICL MANAGED SECURITY OFFERINGS

- **Managed Detection & Response (MDR)** provides full spectrum threat protection through advanced endpoint, identity and network protection, continuous threat analytics and monitoring, weekly threat hunts, and 24/7 incident response. Expert operations infused with threat intelligence further ensure timely and effective threat detection and mitigation.
- **Managed Attack Surface (MAS)** provides continuous visibility into endpoint and infrastructure vulnerabilities, and remediations are prioritized based on risk with expert guidance to accelerate effective response.
- **Managed Security Awareness (MSA)** reduces employee risk through phishing simulations, topical training (e.g., CUI handling), and ongoing training emails.
- **Managed Log Analytics (MLA)** provides centralized collection and retention of audit logs across endpoint, identity, network and other sources, with continuous monitoring for logging failures and on-demand search and reporting to support audit and investigation requirements.
- **Managed Compliance Adherence (MCA)** provides the platform, CCA (CMMC Certified Assessor) guidance, and documentation infrastructure needed to build and sustain compliance across all 110 CMMC Level 2 practices. Continuous evidence collection and expert oversight ensure the program holds up under C3PAO assessment.

CMMC COVERAGE MATRIX

DOMAIN	CONTROL	RADICL CONTROL COVERAGE
Access Control (AC)	AC.L2-3.1.7 Prevent non-privileged users from executing privileged functions and capture the execution of such functions in audit logs.	RADICL's Managed Detection and Response (MDR) offerings monitor remote access and privileged access activity. Identity monitoring surfaces unauthorized access attempts, privilege escalation events, and anomalous authentication activity. Network monitoring confirms remote sessions route through authorized connection points. Log management retains audit records for privileged function activity as assessor-ready evidence.
	AC.L2-3.1.12 Monitor and control remote access sessions.	
Awareness and Training (AT)	AT.L2-3.2.1 Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.	RADICL's Managed Security Awareness (MSA) service delivers and tracks role-based training, continuous phishing simulation, and insider threat awareness content covering CUI handling and reporting obligations. Training completion records, phishing click-rate results, and corrective training assignments are retained as evidence for assessment.
	AT.L2-3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	

DOMAIN	CONTROL	RADICL CONTROL COVERAGE
Audit and Accountability (AU)	AU.L2-3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	RADICL's Managed Log Analytics (MLA) service addresses the core of this domain. Endpoint, identity, and network audit records are collected, retained, and protected against unauthorized modification. Our Security Operations Center (SOC) monitors for audit logging failures and alerts on any detected gap, with on-demand record search available through the RADICL Platform. Management of audit logging functionality is limited to a defined subset of privileged RADICL vSOC personnel and customer defined users.
	AU.L2-3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users so they can be held accountable for their actions.	
	AU.L2-3.3.3 Review and update logged events.	
	AU.L2-3.3.4 Alert in the event of an audit logging process failure.	
	AU.L2-3.3.5 Correlate audit record review, analysis, and reporting processes for investigation and response to indications of unlawful, unauthorized, suspicious, or unusual activity.	
	AU.L2-3.3.6 Provide audit record reduction and report generation to support on-demand analysis and reporting.	
	AU.L2-3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	
Configuration Management (CM)	AU.L2-3.3.9 Limit management of audit logging functionality to a subset of privileged users.	RADICL's endpoint and network monitoring surfaces high-risk or unexpected program execution, and flags activity consistent with unauthorized software installation. Network monitoring identifies traffic anomalies associated with non-essential services, and log management retains the change event record across endpoint and identity sources.
	CM.L2-3.4.7 Restrict, disable, or prevent the use of non-essential programs, functions, ports, protocols, and services.	
Incident Response (IR)	CM.L2-3.4.9 Control and monitor user-installed software.	Incident handling is managed by the RADICL SOC, included in RADICL's MDR offerings, and encompasses detection, analysis, containment, and recovery activities. Every security incident produces timestamped case records with analyst notes, evidence collected, and response actions taken — available as assessment documentation. RADICL's compliance team develops and facilitates incident response tabletop exercises, producing scenario documentation and after-action records.
	IR.L2-3.6.1 Establish an operational incident-handling capability for organizational systems that includes preparation, detection, analysis, containment, recovery, and user response activities.	
	IR.L2-3.6.2 Track, document, and report incidents to designated officials and/or authorities both internal and external to the organization.	
	IR.L2-3.6.3 Test the organizational incident response capability.	
Maintenance (MA)	MA.L2-3.7.4 Check media containing diagnostic and test programs for malicious code before the media are used in organizational systems.	RADICL's Endpoint protection scans files from external media on connection and execution as a standard platform function, addressing the diagnostic media scanning requirement for maintenance activities.

DOMAIN

CONTROL

RADICL CONTROL COVERAGE

Personnel Security (PS)**PS.L2-3.9.2**

Ensure that organizational systems containing CUI are protected during and after personnel actions such as terminations and transfers.

RADICL's MDR offerings monitor user activity across endpoint, identity, and network telemetry. When notified of a personnel action — termination, transfer, or role change — the RADICL vSOC can perform a targeted activity review across the relevant time window, and any unauthorized access, data staging, or unusual file activity associated with the event can be investigated and documented.

Risk Assessment (RA)**RA.L2-3.11.2**

Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified.

RADICL's Managed Attack Surface (MAS) offering identifies vulnerabilities in the environment through continuous authenticated scanning, and takes a risk-based approach to prioritizing them — factoring in exploitability, asset exposure, and available exploit data. Remediation progress is tracked to confirmed closure, with follow-up scanning to detect regression.

RA.L2-3.11.3

Remediate vulnerabilities in accordance with risk assessments.

Security Assessment (CA)**CA.L2-3.12.1**

Periodically assess the security controls in organizational systems to determine if the controls are effective in their application.

RADICL's Managed Compliance Adherence (MCA) offering utilizes the RADICL platform and compliance experts to issue, track, and monitor security control assessments on an ongoing basis. The System Security Plan (SSP) is authored in conjunction with RADICL, describing system boundaries, environments of operation, and how security requirements are implemented — with policies, procedures, evidence, and conformity statements documented within the platform.

CA.L2-3.12.3

Monitor security controls on an ongoing basis to ensure the continued effectiveness of the controls.

CA.L2-3.12.4

Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationship with or connection to other systems.

System and Information Integrity (SI)**SI.L1-3.14.1**

Identify, report, and correct system flaws in a timely manner.

RADICL leverages best-in-breed, compliant Endpoint Detection and Response (EDR) tools, combined with Managed Attack Surface scanning, to identify flaws, malicious code, security alerts, inbound and outbound communications, and unauthorized use of organizational systems. These tools receive real-time updates of code protection mechanisms and perform continuous real-time scanning of all files and processes on protected systems. When malicious files, processes, or activities are identified, appropriate remediation actions (such as file quarantine, process kill, and network quarantine) are performed.

SI.L1-3.14.2

Provide protection from malicious code at designated locations within organizational systems.

SI.L1-3.14.3

Monitor system security alerts and advisories and act in response.

SI.L1-3.14.4

Update malicious code protection mechanisms when new releases are available.

SI.L1-3.14.5

Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed.

SI.L1-3.14.6

Monitor organizational systems, including inbound and outbound communications traffic, to detect attacks and indicators of potential attacks.

SI.L2-3.14.7

Identify unauthorized use of organizational systems.

RADICL MANAGED SECURITY OFFERINGS

The following matrix identifies the specific RADICL product providing full or partial control coverage.

DOMAIN	CONTROL	MDR Endpoint	MDR Identity	MDR Network	MAS	MSA	MLA	MCA
Access Control (AC)	AC.L2-3.1.7	●	●					
	AC.L2-3.1.12	●	●					
Awareness and Training (AT)	AT.L2-3.2.1					●		
	AT.L2-3.2.3					●		
Audit and Accountability (AU)	AU.L2-3.3.1	●	●	●			●	
	AU.L2-3.3.2	●	●				●	
	AU.L2-3.3.3	●	●	●			●	
	AU.L2-3.3.4	●	●	●			●	
	AU.L2-3.3.5	●	●	●			●	
	AU.L2-3.3.6	●	●	●			●	
	AU.L2-3.3.8	●	●	●			●	
	AU.L2-3.3.9	●	●	●			●	
Configuration Management (CM)	CM.L2-3.4.7	●	●	●				
	CM.L2-3.4.9	●						
Incident Response (IR)	IR.L2-3.6.1	●	●	●				
	IR.L2-3.6.2	●	●	●				
	IR.L2-3.6.3					●		
Maintenance (MA)	MA.L2-3.7.4	●						
Personnel Security (PS)	PS.L2-3.9.2		●					
Risk Assessment (RA)	RA.L2-3.11.2	●			●			
	RA.L2-3.11.3	●			●			
Security Assessment (CA)	CA.L2-3.12.1							●
	CA.L2-3.12.3							●
	CA.L2-3.12.4							●
System and Information Integrity (SI)	SI.L1-3.14.1	●			●			
	SI.L1-3.14.2	●						
	SI.L2-3.14.4	●						
	SI.L2-3.14.3	●						
	SI.L2-3.14.5	●						
	SI.L2-3.14.6	●		●				
	SI.L2-3.14.7	●	●	●				

CONCLUSION

RADICL's managed compliance and security offerings help companies of all sizes accelerate and ensure fast CMMC readiness. Using the full platform provides near immediate realization of many hard-to-meet compliance requirements with an expert-guided pathway to complete readiness. Fast track your CMMC journey and reduce your risk of ransomware, data theft, and other high impact cyber incidents.