RADICL™

CMMC Level 2 Control Coverage

CMMC Level 2 is based on NIST SP 800-171 Rev2 and consists of 110 controls across 14 domains. RADICL's Managed Compliance Adherence (MCA) offering helps prepare organizations for CMMC assessment by guiding the implementation of NIST SP 800-171 Rev2 in its entirety. RADICL's managed security offerings provide additional compliance support, directly addressing 29 of the most costly and difficult to implement controls, further accelerating compliance across 10 domains.

RADICL Managed Security Offerings

Managed Detection and Response (MDR) provides full spectrum threat protection through advanced endpoint 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. Vulnerability remediations are prioritized based on risk with expert guidance accelerating effective response.

Managed Security Awareness (MSA) provides enhanced security awareness through annual training, topical training (e.g., CUI handling), and ongoing training emails. Phishing simulations and corrective training further reduce employee risk.

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 help monitor remote access as well as privileged access. Execution of functions, local and remote authentication, and file access events are monitored, and threat hunts and custom detection analytics alert on installation and use of remote access tools. VPN authentication sessions are monitored as well as cloud-based identity, authentication and SSO providers such as Entra ID, with custom threat hunts and detection analytics in place designed to identify anomalous or malicious activity.
	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) provides role-based security awareness training courses meeting CMMC requirements. In addition, MSA includes continuous phishing simulation exercises as well as biweekly e-mail-based training tidbits to ensure security awareness remains top-of-mind for end-users throughout the entire training cycle.
	AT.L2-3.2.2 Ensure that personnel are trained to carry out their assigned information security-related duties and responsibilities.	
	AT.L2-3.2.3 Provide security awareness training on recognizing and reporting potential indicators of insider threat.	
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 retains audit logs needed to enable the monitoring, analysis, investigation and reporting of unlawful or unauthorized activities. RADICL collects and retains logs from endpoints, cloud infrastructure, network infrastructure, and application infrastructure. These logs support the ability to trace users to their actions, and are continuously reviewed and monitored 24x7 for audit logging failures, and unlawful, suspicious or unusual activity by the RADICL vSOC through threat hunting and real time detection rules. The logs can also be searched and reported on in the RADICL platform, and are protected in the RADICL platform from unauthorized access, modification and deletion.
	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)	**CM.L2-3.4.7** Restrict, disable, or prevent the use of nonessential programs, functions, ports, protocols, and services.	During onboarding, RADICL builds a baseline of authorized endpoint and network activity. Built-in EDR detection analytics are tuned and combined with RADICL's custom analytics to detect and prevent the use of nonessential and unauthorized programs, and network traffic is monitored for suspicious or unauthorized activity. Identified potentially unwanted programs and activity are quarantined and removed through RADICL platform-driven tasks.
	CM.L2-3.4.9 Control and monitor user-installed software.	
Incident Response (IR)	**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.	Incident handling requirements are primarily managed by the RADICL vSOC. This service is included in RADICL's MDR offerings, and encompasses the detection, analysis, containment, and recovery activities. All required Incident Response documentation, testing and exercise can also be delivered by RADICL.
	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.	
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 all user activity. When notified of a personnel action such as a termination or transfer, the RADICL vSOC will perform additional reviews of the user's activities during the periods leading up to and after the personnel action, and any suspicious or unauthorized activity is investigated.
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 offering identifies vulnerabilities in the environment, and takes a risk-based approach to prioritizing them. Factors such as exploitability, vulnerability location, and availability of an exploit are taken into account when assessing the risk of a vulnerability.
	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 offering utilizes the RADICL platform and compliance experts to issue, track, and validate security control assessments. Assessments include the requirement to document policies, procedures, evidence, and conformity statements, all within the platform.
System & Communications Protection (SC)	**SC.L1-3.13.1** Monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.	RADICL's MDR offerings monitor, investigate, and respond to endpoint, network and cloud alerts for suspicious or unauthorized communications.
System & 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 to identify flaws, malicious code, security alerts, inbound and outbound communications and unauthorized use of organizational systems. These EDR 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 a host 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 Product Coverage Matrix

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

Domain	Control	MDR Managed Detection & Response			MAS Managed Attack Surface	MSA Managed Security Awareness	MCA Managed Compliance Adherence
		Endpoint	Identity	Network			
Access Control (AC)	AC.L2-3.1.7	●	●				
	AC.L2-3.1.12	●	●	●			
Awareness and Training (AT)	AT.L2-3.2.1					●	
	AT.L2-3.2.2					●	
	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	●	●	●			
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	●	●	●			
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						●

Domain	Control	MDR Managed Detection & Response			MAS Managed Attack Surface	MSA Managed Security Awareness	MCA Managed Compliance Adherence
		Endpoint	Identity	Network			
System and Communications Protection (SC)	SC.L1-3.13.1	●	●	●			
System & Information Integrity (SI)	SI.L1-3.14.1	●			●		
	SI.L1-3.14.2	●					
	SI.L1-3.14.3	●					
	SI.L1-3.14.4	●					
	SI.L1-3.14.5	●					
	SI.L1-3.14.6	●					
	SI.L1-3.14.7	●					

Conclusion

Companies that seek to accelerate and ensure fast CMMC readiness should consider leveraging RADICLs managed compliance and security offerings. The combination of both provides near immediate realization of many hard-to-meet requirements with an expert driven pathway to complete readiness. With the full RADICL offering, you can fast track your CMMC journey and immediately reduce your risk of ransomware, data theft and other high impact cyber incidents.