

NIST CSF 2.0 SUBCATEGORY COVERAGE

NIST CSF 2.0 organizes cybersecurity outcomes into 106 Subcategories across six Functions (Govern, Identify, Protect, Detect, Respond, and Recover). RADICL's Managed Compliance Adherence (MCA) guides organizations through building a documented Profile against the framework in its entirety, while. RADICL's managed security offerings provide additional operational coverage, **directly operating 45 of the most operationally demanding Subcategories, and extending coverage across all six Functions.**

RADICL Managed Security Offerings

- **Managed Detection & 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, 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, correlation, and retention of audit logs across endpoint, identity, and network sources, with continuous monitoring for logging failures and on-demand search and reporting to support audit and investigation requirements.
- **Managed Compliance Adherence (MCA)** gives you clear, trackable steps toward compliance frameworks such as NIST 800-171 and CMMC, with hands-on consulting from our team of compliance experts and a unified dashboard for full and continuous visibility.

NIST CSF 2.0 Coverage Matrix

FUNCTION	SUBCATEGORY	RADICL SUBCATEGORY COVERAGE
Govern (GV)	GV.RR-03 Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies.	RADICL functions as the flexible security staffing your risk strategy calls for, scaling coverage up or down as risk changes, and as the critical security supplier your incident plan names — actively coordinating incident planning, response, and recovery activities alongside your team and any other named third parties.
	GV.SC-08 Relevant suppliers and other third parties are included in incident planning, response, and recovery activities.	
Identify (ID)	ID.AM-01 Inventories of hardware managed by the organization are maintained.	RADICL's Managed Attack Surface (MAS) and Managed Detection and Response (MDR) offerings continuously discover new hardware joining the environment, identify and validate vulnerabilities, and pull in cyber threat intelligence on who and what is targeting the organization. Findings feed a shared risk response process so RADICL and your team can jointly select, prioritize, and track responses. Every after-action review, test, and exercise produces documented improvements to the plans and procedures that keep the program current.
	ID.RA-01 Vulnerabilities in assets are identified, validated, and recorded.	

FUNCTION

SUBCATEGORY

RADICL SUBCATEGORY COVERAGE

ID.RA-02

Cyber threat intelligence is received from information sharing forums and sources.

ID.RA-03

Internal and external threats to the organization are identified and recorded.

ID.RA-05

Threats, vulnerabilities, likelihoods, and impacts are used to understand inherent risk and inform risk response prioritization.

ID.RA-06

Risk responses are chosen, prioritized, planned, tracked, and communicated.

ID.IM-01

Improvements are identified from evaluations.

ID.IM-02

Improvements are identified from security tests and exercises, including those done in coordination with suppliers and relevant third parties.

ID.IM-03

Improvements are identified from execution of operational processes, procedures, and activities.

ID.IM-04

Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved.

**Protect
(PR)****PR.AT-01**

Personnel are provided with awareness training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind.

PR.PS-02

Software is maintained, replaced, and removed commensurate with risk.

PR.PS-04

Log records are generated and made available for continuous monitoring.

PR.PS-05

Installation and execution of unauthorized software are prevented.

RADICL's Managed Security Awareness (MSA) delivers and tracks general cybersecurity awareness training organization-wide. Managed Attack Surface (MAS) discovers and prioritizes outdated or vulnerable software so your team knows what to patch first. Managed Detection and Response (MDR) enforces application control on protected endpoints, and Managed Log Analytics (MLA) confirms the log records needed for continuous monitoring are generated and retained.

**Detect
(DE)****DE.CM-01**

Networks and network services are monitored to find potentially adverse events.

DE.CM-03

Personnel activity and technology usage are monitored to find potentially adverse events.

DE.CM-06

External service provider activities and services are monitored to find potentially adverse events.

This is the core of RADICL's Managed Detection and Response (MDR) offering. Our vSOC continuously monitors network traffic, personnel and technology usage, external service provider activity, and computing hardware, software, and runtime environments to find potentially adverse events. Every event is analyzed, correlated across sources, scoped for impact, enriched with threat intelligence, and (when it meets defined criteria) declared as an incident with full documentation.

FUNCTION	SUBCATEGORY	RADICL SUBCATEGORY COVERAGE
Respond (RS)	DE.CM-09 Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events.	RADICL's vSOC executes the full incident response lifecycle: triaging and validating reports, categorizing and prioritizing incidents, escalating as needed, and coordinating execution of the response plan with relevant third parties. Analysis establishes what happened and the root cause, with all actions, data, and metadata preserved with integrity. Internal and external stakeholders are notified and kept informed throughout, while containment and eradication are performed directly by the vSOC.
	DE.AE-02 Potentially adverse events are analyzed to better understand associated activities.	
	DE.AE-03 Information is correlated from multiple sources.	
	DE.AE-04 The estimated impact and scope of adverse events are understood.	
	DE.AE-06 Information on adverse events is provided to authorized staff and tools.	
	DE.AE-07 Cyber threat intelligence and other contextual information are integrated into the analysis.	
	DE.AE-08 Incidents are declared when adverse events meet the defined incident criteria.	
	RS.MA-01 The incident response plan is executed in coordination with relevant third parties once an incident is declared.	
	RS.MA-02 Incident reports are triaged and validated.	
	RS.MA-03 Incidents are categorized and prioritized.	
	RS.MA-04 Incidents are escalated or elevated as needed.	
	RS.MA-05 The criteria for initiating incident recovery are applied.	
	RS.AN-03 Analysis is performed to establish what has taken place during an incident and the root cause of the incident.	
	RS.AN-06 Actions performed during an investigation are recorded, and the records' integrity and provenance are preserved.	
	RS.AN-07 Incident data and metadata are collected, and their integrity and provenance are preserved.	
	RS.AN-08 An incident's magnitude is estimated and validated.	
	RS.CO-02 Internal and external stakeholders are notified of incidents.	

FUNCTION	SUBCATEGORY	RADICL SUBCATEGORY COVERAGE						
Recover (RC)	RS.CO-03 Information is shared with designated internal and external stakeholders.							
	RS.MI-01 Incidents are contained.							
	RS.MI-02 Incidents are eradicated.							
	RC.RP-01 The recovery portion of the incident response plan is executed once initiated from the incident response process.							
	RC.RP-02 Recovery actions are selected, scoped, prioritized, and performed.							
	RC.RP-03 The integrity of backups and other restoration assets is verified before using them for restoration.							
	RC.RP-05 The integrity of restored assets is verified, systems and services are restored, and normal operating status is confirmed.							
	RC.RP-06 The end of incident recovery is declared based on criteria, and incident-related documentation is completed.							
	RC.CO-03 Recovery activities and progress in restoring operational capabilities are communicated to designated internal and external stakeholders.							

RADICL Product Coverage Matrix

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

FUNCTION	SUBCATEGORY	MDR Endpoint	MDR Identity	MDR Network	MAS	MSA	MLA	MCA
Govern (GV)	GV.RR-03	●	●	●	●	●	●	●
	GV.SC-08	●	●	●				●
Identify (ID)	ID.AM-01	●						
	ID.RA-01				●			
	ID.RA-02	●		●				
	ID.RA-03	●	●	●	●			
	ID.RA-05				●			●
	ID.RA-06				●			●
	ID.IM-01							●
	ID.IM-02	●	●	●				●
	ID.IM-03	●	●	●				
	ID.IM-04	●	●	●				●

FUNCTION	SUBCATEGORY	MDR Endpoint	MDR Identity	MDR Network	MAS	MSA	MLA	MCA
Protect (PR)	PR.AT-01					●		
	PR.PS-02				●			
	PR.PS-04						●	
	PR.PS-05	●						
Detect (DE)	DE.CM-01			●				
	DE.CM-03	●	●					
	DE.CM-06		●				●	
	DE.CM-09	●						
	DE.AE-02	●	●	●				
	DE.AE-03	●	●	●			●	
	DE.AE-04	●	●	●				
	DE.AE-06	●	●	●			●	
	DE.AE-07	●	●	●				
	DE.AE-08	●	●	●				
Respond (RS)	RS.MA-01	●	●	●				
	RS.MA-02	●	●	●				
	RS.MA-03	●	●	●				
	RS.MA-04	●	●	●				
	RS.MA-05	●	●	●				
	RS.AN-03	●	●	●				
	RS.AN-06	●	●	●			●	
	RS.AN-07						●	
	RS.AN-08	●	●	●				
	RS.CO-02	●	●	●				
	RS.CO-03	●	●	●				
	RS.MI-01	●		●				
	RS.MI-02	●						
Recover (RC)	RC.RP-01	●	●	●				
	RC.RP-02	●	●	●				
	RC.RP-03	●						
	RC.RP-05	●						
	RC.RP-06	●	●	●				
	RC.CO-03	●	●	●				

Conclusion

RADICL's managed compliance and security offerings help organizations of all sizes professionalize their cybersecurity program. MCA guides your team in building a documented Profile against the full NIST CSF framework, while RADICL's managed security offerings directly operate the Subcategories that demand ongoing execution. With the full RADICL Platform, you build the trust your board, employees, and customers expect, and materially reduce your risk of ransomware, data theft, and other high-impact cyber incidents.