

CYBERSECURITY-AS-A-SERVICE

BUILD THE PROGRAM. OPERATE THE CONTROLS.

Trust isn't something you claim — it's something you prove. Adhering to a recognized framework like NIST CSF 2.0 is how you show your board, your employees, and your customers that cybersecurity isn't an afterthought. RADICL builds and operates that program from the ground up, so you're not crossing your fingers hoping to dodge an incident. With us, you know you're protected.

106

BUILD

MANAGED COMPLIANCE ADHERENCE (MCA)

NIST CSF 2.0 organizes cybersecurity outcomes across 106 Subcategories spanning six Functions (Govern, Identify, Protect, Detect, Respond, and Recover). MCA gives you the platform and expert guidance to help your team build a program you can reliably stand behind.

- **Platform** — Centralized control for policies, procedures, evidence, and your Current and Target Profiles, giving reviewers everything they need in one place.
- **Readiness** — Expert-guided review across all six Functions, with hands-on evaluation to confirm implementation evidence, expose hidden gaps, and work with you to build a prioritized roadmap to your Target Profile.
- **Docs** — Current Profile, Target Profile, gap assessment, and improvement roadmap — developed together with your team, structured to NIST CSF 2.0 and purpose-built for your environment.
- **Expert support** — Dedicated compliance team advises on what a mature profile looks like before you're asked to show one to a customer, prime, or underwriter.

Program-Wide · All 6 Functions

45

OPERATE

MDR · MAS · MSA · MLA

RADICL CSaaS performs ongoing cybersecurity work across 45 of the 106 CSF Subcategories to — running managed detection and response, vulnerability management, incident response, and security awareness directly, and extend continuous monitoring across the tools your IT team or MSP already run. You get direct operational coverage, not 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 ready-made artifacts from every event.
- **Security awareness** — Annual training, phishing simulation, and custom content covering CUI handling and insider threat recognition.

45 of 106 Subcategories

KNOW EXACTLY WHO COVERS WHAT, BEFORE ANYONE ASKS

Every RADICL engagement includes a Shared Responsibility Matrix (SRM), a documented breakdown of which CSF Subcategories RADICL actively operates, which are shared, and which belong to your organization. There's no room forNo ambiguysurprises, and. No surprises confusion when a customer, prime, or underwriter asks who owns what.

106

NIST CSF 2.0
SUBCATEGORIES MAPPED

COVERAGE IN PRACTICE

NIST CSF 2.0 expects evidence of implementation, whether you're using it to answer a customer questionnaire, apply for cyber insurance, or report to your board. Below are representative Subcategories from each coverage layer showing what RADICL does and what your organization still owns.

BUILD

MCA provides the platform, guidance, and documentation to address these Subcategories. Our compliance experts help you build the profile artifacts your customers, primes, and underwriters want to see.

GV.RM-03

Cybersecurity risk management activities and outcomes are included in enterprise risk management processes

WHAT NIST CSF REQUIRES

A documented connection between the cybersecurity risk register and the organization's broader enterprise risk process, with evidence that cyber risk is weighed in business decisions, — not managed off to the side.

HOW MCA ADDRESSES IT

MCA's Readiness phase guides your team through building a risk register and tying cybersecurity risk directly into your enterprise risk process. Our compliance experts work alongside you to document how identified risks are evaluated, escalated, and revisited, so you walk away with the governance artifacts a customer or board review expects to see.

ID.RA-04

Potential impacts and likelihoods of threats exploiting vulnerabilities are identified and recorded

WHAT NIST CSF REQUIRES

A documented risk assessment methodology, an up-to-date risk register recording likelihood and impact for identified threats, and evidence the register is reviewed on a defined cadence.

HOW MCA ADDRESSES IT

RADICL's compliance team works with you to build and maintain the risk register, scoring likelihood and impact together for identified threats and vulnerabilities. The register lives in the Platform, versioned and ready whenever a customer or underwriter asks how you evaluate risk.

PR.AA-03

Users, services, and hardware are authenticated commensurate with the risk of the transaction

WHAT NIST CSF REQUIRES

A documented authentication policy (— including where multi-factor authentication is required based on risk), — implementation evidence across 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 Subcategory. Our experts flags policies running in report-only mode, works with you to document which user populations are in scope, and produces a conformity statement tied to the outcome. Policy, procedure, and evidence are fully managed in the Platform.

PR.DS-01

The confidentiality, integrity, and availability of data-at-rest are protected

WHAT NIST CSF REQUIRES

A documented data protection policy identifying where sensitive data lives, what encryption or access controls protect it at rest, and evidence those controls are applied across in-scope systems.

HOW MCA ADDRESSES IT

MCA's Docs component works with you to inventory where sensitive data is stored and document the protections in place, such as — encryption, access restrictions, and storage location. Our team confirms the written policy matches what's actually configured before it's included in your Profile.

OPERATE

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

RADICL actively operates coverage for these Subcategories. The vSOC runs the required people, process, and technology so your organization doesn't have to.

DE.CM-01

Networks and network services are monitored to find potentially adverse events

WHAT NIST CSF REQUIRES

Continuous monitoring of network traffic and services with a documented detection capability and evidence of active response when adverse events are identified.

HOW RADICL OPERATES IT

MDR for Network runs 24/7. Built-in and custom detection analytics monitor all network traffic. Each detection generates a vSOC case with full event documentation you can point to as evidence.

RS.MA-01

The incident response plan is executed once an incident is declared

WHAT NIST CSF REQUIRES

A documented incident response plan and evidence that it's followed when something happens — not just filed away, but executed with a recorded timeline.

HOW RADICL OPERATES IT

The vSOC opens, tracks, and closes cases in the RADICL Platform the moment an incident is declared. Every incident has a full event timeline, analyst notes, and closure documentation, directly available as evidence your plan works.

ID.RA-01

Vulnerabilities in assets are identified, validated, and recorded

WHAT NIST CSF REQUIRES

Defined scanning frequency, evidence scans are run on schedule, and a validated, recorded list of vulnerabilities.

HOW RADICL OPERATES IT

MAS runs continuous vulnerability scans across enrolled assets. Findings are validated, prioritized, and tracked to closure, with rescans to confirm remediation and automatically flag regressions.

PR.AT-01

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

WHAT NIST CSF REQUIRES

A documented training program with evidence that personnel complete general cybersecurity awareness training on a defined cadence.

HOW RADICL OPERATES IT

MSA delivers and tracks annual training and phishing simulation for your whole organization. Completion records and phishing results are maintained in the Platform as ready-made evidence.