RADICL™

Platform-Guided Assessments, Workflows & Audit Assurance

ROOTED IN SECURITY
EXPERTS IN NIST CSF COMPLIANCE

RADICL HELPS SIMPLIFY, ACCELERATE, AND REDUCE THE COST OF NIST CSF COMPLIANCE

The NIST Cybersecurity Framework (CSF) is the standard mature organizations use to demonstrate structured, disciplined security. SMBs now face the same sophisticated threats as large enterprises, from ransomware gangs to nation-state actors, and stakeholders increasingly expect proof of enterprise-grade security practices. NIST CSF provides that proof, showing you manage cybersecurity risk with rigor and accountability, not just ad-hoc responses.

NIST CSF is not a binder or a one-time audit. It is an operating model. Implementing it correctly, and maintaining alignment over time, requires expertise and attention most small teams simply can't set aside while running their business.

OUR MISSION

We protect American small businesses who are high value targets for cyber criminals. We materially reduce their cyber incident risk by operationalizing frameworks like NIST CSF so customers can prove to others, and believe themselves, that cybersecurity is being done the right way.

RADICL's Managed Compliance Adherence service does the heavy lift of NIST CSF 2.0 for you. We identify posture gaps, guide customers through foundational controls, and help organizations maintain ongoing alignment so your environment actually runs to NIST, not just claims to.

You get enterprise-grade operating discipline without hiring a security team or becoming a NIST expert. The outcome isn't documentation and a to-do-list it's operationalized best practices driving management and board confidence that your company is secure.

THE BASICS OF NIST CSF 2.0:

If you're new to NIST CSF, here's what you need to know:

PURPOSE: The primary purpose of NIST CSF is to provide organizations with a voluntary framework for managing and reducing cybersecurity risk. The framework helps organizations communicate about cybersecurity risk management and improve their cybersecurity posture through foundational security controls.

FRAMEWORK FUNCTIONS: NIST CSF 2.0 defines six core functions of cybersecurity: Govern, Identify, Protect, Detect, Respond, and Recover. Organizations implement practices within each function based on their risk tolerance and business requirements, establishing baseline security controls.

IMPLEMENTATION FLEXIBILITY: Organizations can use NIST CSF at various maturity levels, from basic implementations to advanced programs. The framework supports risk-based approaches allowing organizations to optimize scope and prioritize activities based on their unique business and risk considerations.

SUBCATEGORIES & OUTCOMES: NIST CSF 2.0 covers 106 subcategories across 6 functions and 23 categories. These subcategories define desired cybersecurity outcomes including asset management, vulnerability management, incident response, security awareness training, and continuous monitoring that can be mapped to specific security controls in implementation standards.

CONTINUOUS IMPROVEMENT: NIST CSF emphasizes continuous improvement and regular assessment. Organizations must maintain and enhance their cybersecurity practices to address evolving threats and business changes through ongoing monitoring.

THE RADICL COMPLIANCE EXPERIENCE

PLATFORM ONBOARDING

Your IT team (and MSP, if applicable) will be onboarded to the RADICL platform. Your compliance program is driven through our platform with expert guidance, full transparency, and in-app collaboration.

ASSESSMENT

RADICL guides a comprehensive assessment of your current compliance across all 106 CSF subcategories, clarifying exactly where you stand today.

GUIDED REMEDIATION

RADICL expertly guides, and when possible automates, compliance with CSF best practices. Practical decisions can be made along the way, balancing risk against the implementation and operational costs of adherence.

EVIDENCE CAPTURE

Throughout assessment and remediation, notes, screenshots, and files are easily captured and automatically organized, ensuring management and auditors can validate work performed and decisions made.

AI ASSISTANCE

RADICL's AI agent, Jett, is ready to help you along the way by clarifying hard to define requirements or generating documentation to accelerate your journey.

POSTURE VISIBILITY

Real-time dashboards provide up-to-date visibility into progress and overall compliance posture, keeping leadership informed throughout the process.

WHY RADICL?

EXPERT-GUIDED AUTOMATION

Certified compliance experts combined with AI-powered workflows means you get the speed of automation with the judgment of experienced professionals—not just a software tool.

SECURITY + COMPLIANCE, INTEGRATED

RADICL comprehensive Cybersecurity-as-a-Service (CSaaS) offering directly addresses up to 106 NIST CSF controls, bringing fast compliance adherence in areas most critical to incident avoidance such as vulnerability management, security awareness training and 24/7 managed detection and response.

SCOPE OPTIMIZATION

We help you focus compliance efforts on what actually matters for your business, balancing risk against implementation costs, not forcing you to gold-plate everything.

AUDIT-READY

Evidence capture, centralized documentation, and real-time posture visibility means you're always prepared, not scrambling when assessors show up.