RiskWatch

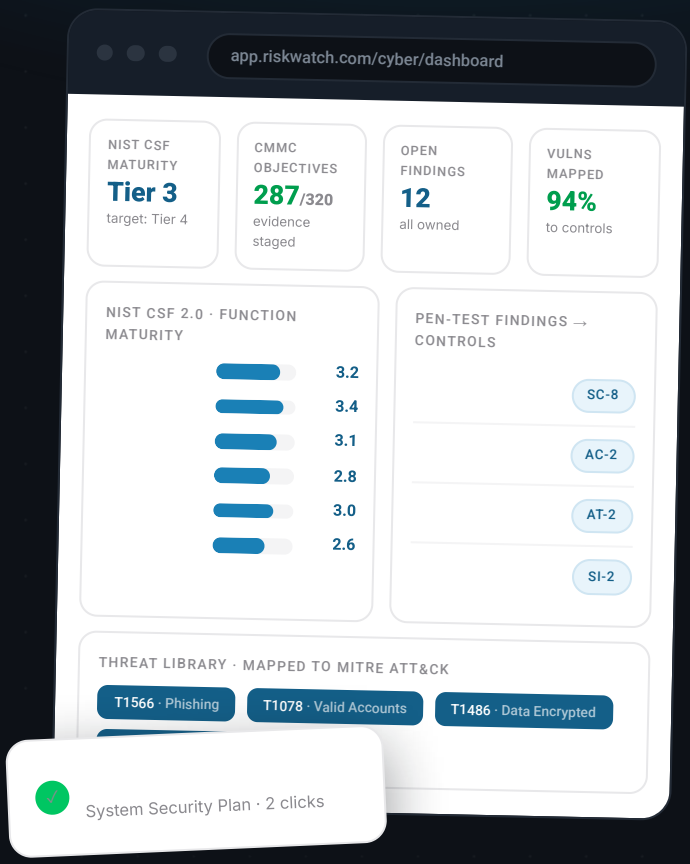
CYBER SECURITY RISK MANAGEMENT

CYBER RISK MANAGEMENT SOFTWARE

From pen-test PDF to control-level finding.

Cyber maturity scoring aligned to NIST CSF 2.0, CIS Controls, and ISO 27001:2022. A threat library mapped to MITRE ATT&CK, vulnerability workflow integration, and cyber-to-compliance reporting: one cyber assessment maps to SOC 2, ISO 27001, and NIST 800-53 controls.

NIST CSF 2.0 | MITRE ATT&CK | CMMC-READY | VULNERABILITY WORKFLOW | CYBER-TO-COMPLIANCE | MATURITY SCORING



500+
compliance and risk teams

40+
regulatory frameworks

Since 1993
30+ years in assessments

Audited
SOC 2 Type II · ISO/IEC 27001:2022

THE REALITY

The same NIST CSF gap analysis, redone from scratch every year.

Maturity in one tool, evidence in another, pen-tests in PDFs. If two of these six cards describe your program, the platform pays for itself.

Two tools, one program

SOC 2 evidence lives in one tool, the NIST CSF maturity assessment in another. Neither knows the other exists.

320 objectives, one audit

The CMMC C3PAO is coming and every assessment objective needs staged evidence. Spreadsheet tracking breaks at about 50.

Pen-tests die in PDFs

The findings are real, the report is thorough, and none of it maps to controls. Next year's test finds the same things.

Cyber risk, off the register

Cyber findings never reach the enterprise risk register, so the board sees cyber as a separate universe. It isn't.

Vulns without context

The scanner finds 4,000 vulnerabilities. Which ones break a control you attested to last quarter? Nobody can say.

The annual groundhog day

Every year the NIST CSF gap analysis starts from a blank workbook, because last year's lives in a consultant's archive.

FROM FRAMEWORK TO BOARD-READABLE SCORE

DAY 1

Pick the frameworks

NIST CSF 2.0 by default. Add CMMC 2.0, NIST 800-171 r3, ISO 27001, SOC 2, or your own. Cross-mapped from the start.

WEEK 1

Assess maturity

Survey-based assessment scores maturity per function and tier. One rubric, comparable across years and entities.

CONTINUOUS

Map findings to controls

Pen-test findings, scanner output, and incidents land on the controls they break. Remediation runs as tracked tasks.

ON-DEMAND

Report cyber-to-compliance

One cyber assessment maps to SOC 2, ISO 27001, and NIST 800-53 controls. NIST SSP and CMMC SPRS export in two clicks.

THE NIST LIBRARY, BUILT IN

NIST CSF 2.0 · NIST SP 800-53 r5 · NIST SP 800-171 r3 · NIST SP 800-66 · NIST AI RMF · CMMC 2.0 · FedRAMP · FISMA

Watch the 4-minute platform tour at **riskwatch.com/cyber-security-assessment-software** →

CYBER-TO-COMPLIANCE

One cyber assessment. Every framework's controls.

Cross-mapping turns a single cyber assessment into control evidence for every framework that references it. No re-assessment, no duplicate evidence.

One cyber assessment

maturity scored · findings mapped · evidence attached

NIST 800-53 r5

control families, SSP-ready

CMMC 2.0

pre-mapped to 800-171 r3 · SPRS export

SOC 2 Type II

security trust criteria

ISO/IEC 27001:2022

Annex A controls

+ FedRAMP and FISMA

Maturity scoring

NIST CSF 2.0 tiers across all six functions. CIS Controls and ISO 27001:2022 alignment included.

Threat library

Pre-loaded threats mapped to MITRE ATT&CK techniques where applicable.

Vulnerability workflow

Scanner output feeds the assessment via REST API. Vulns land on the controls they break.

Pen-test-to-control

Findings map to control statements, get owners and due dates, and stay visible until closed.

CMMC evidence staging

Every assessment objective tracks its evidence. SPRS score export when you're ready.

Cyber feeds the register

Cyber findings flow into the enterprise Global Register, so the board sees one risk picture.

Audit pack export

NIST SSP, CMMC SPRS, SOC 2 system description, ISO Statement of Applicability. Two clicks.

Integrations

Jira, ServiceNow, Slack, Teams, Power BI, Tableau. REST API with OAuth 2.0 and webhooks.

Built on the NIST stack.

Practitioner-built libraries for the full NIST family, maintained as revisions ship. Originally built for federal-agency assessors.

1. **NIST CSF 2.0 scoring**
   Maturity tiers across Govern, Identify, Protect, Detect, Respond, Recover.
2. **CMMC pre-mapping**
   CMMC L1/L2/L3 pre-mapped to NIST 800-53 r5 and NIST 800-171 r3 controls.
3. **SSP and SPRS in two clicks**
   NIST System Security Plan and CMMC SPRS exports generate from the live record.
4. **The wider NIST family**
   NIST SP 800-66 for HIPAA security and NIST AI RMF for AI governance programs.

60-80%
less duplicate evidence work in multi-framework programs

320
CMMC assessment objectives, pre-mapped and evidence-tracked

40+
frameworks cross-mapped from one assessment

30 days
median implementation with a named CSM

Scan to start the 30-day free trial

IMPLEMENTATION

Live in 30 days, not next quarter.

WEEK 1 · PHASE 1

Scoping

Frameworks, entities, and scanner feeds mapped with your named CSM. No outsourced discovery.

WEEK 2-3 · PHASE 2

Configuration

NIST libraries loaded, cross-mappings applied, vulnerability feeds connected, owners assigned, SSO live.

WEEK 4 · PHASE 3

Pilot and go-live

First maturity assessment runs on real controls. 30-day median implementation; 60 to 90 days multi-entity.

ALWAYS

Named CSM included

The engineer who answers your email is the engineer who answers your phone call. Most tickets resolve in 4 hours.

We hold ourselves to the frameworks we sell.

RiskWatch holds the same kind of evidence customers trust us to manage: assessment scores, control attestations, regulator-facing artifacts. It's protected the way your auditors expect, independently audited, encrypted in transit and at rest, segmented by tenant.

SOC 2 TYPE II · ISO/IEC 27001:2022 · US-EAST RESIDENCY · EU-FRANKFURT RESIDENCY · SAML SSO

"Very user friendly and not spreadsheet based. We think it is a good and useful software application."

TE Connectivity · manufacturing · verified customer review

CMMC, PRE-MAPPED

CMMC 2.0 Levels 1 to 3 ship pre-mapped to NIST SP 800-53 r5 and NIST SP 800-171 r3 controls, with per-objective evidence tracking and SPRS export.

SECURITY TEAMS RUN ON RISKWATCH

Pfizer · Coca-Cola · BOSE · TE · RSI · SECUVANT

30 minutes, live, no slides.

We protect that timebox, Q&A as we go, and we don't gate the demo by title or pre-qualify your team. Bring your NIST CSF target tier and the audit on your calendar.

PRIMARY
Request a demo

TRY IT
Start 30-day free trial

PRICING
Get a quote

Scan to book your demo

RiskWatch

riskwatch.com/cyber-security-assessment-software
1-800-360-1898
sales@riskwatch.com

RiskWatch International LLC · Sarasota, FL
SOC 2 Type II · ISO/IEC 27001:2022 audited