SmartSuite

Framework / Cybersecurity / Other

CRI Profile (Cyber Risk Institute)

The CRI Profile is a voluntary cyber risk framework for financial institutions, built on NIST CSF 2.0, with 318 diagnostic statements, four impact tiers and about 40 regulatory mappings.



What it is

The CRI Profile is a cyber and technology risk management framework for financial institutions, published by the Cyber Risk Institute (CRI), a not-for-profit standards organization in Washington, D.C. It is built on the NIST Cybersecurity Framework, has been aligned to CSF 2.0 since version 2.0 in February 2024, and is now at version 2.2 (April 30, 2026). Use is voluntary: no regulator mandates it.

At a glance

PUBLISHER
Cyber Risk Institute

TYPE
Guidance

VERSION
CRI Profile v2.2 (aligned to NIST CSF 2.0)

EFFECTIVE
Voluntary; no mandated date. Current version 2.2 released April 30, 2026

DOMAIN
Cybersecurity

FAMILY
Other

REGION
International (published in the United States)

INDUSTRY
Financial Services

ADOPTION MODEL
Voluntary

IMPLEMENTATION COMPLEXITY
High

Source: cyberriskinstitute.org/cri-profile-overview/

Why it matters

- **One assessment for many supervisors** The Profile maps its diagnostic statements to about 40 regulatory references and standards, among them NYDFS Part 500, the EU's DORA and the CISA Cybersecurity Performance Goals, so one set of answers can serve several examiners.
- **Expectations scale with impact** Nine questions place an institution in one of four Impact Tiers, and version 2.0 applies 318 diagnostic statements to Tier 1, 311 to Tier 2, 282 to Tier 3 and 208 to Tier 4.
- **Governance and third parties are named functions** The Govern function follows NIST CSF 2.0, and CRI's own Extend function carries third-party lifecycle management, so supplier risk has its own place in the assessment.
- **Evidence is part of the assessment** Each diagnostic statement has explanatory guidance, examples of commonly used artifacts, and fields for the rating, the rationale and the supporting evidence.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports CRI Profile

Impact Tier and Applicability

Record the tier from the nine-question questionnaire and mark each of the diagnostic statements as To Be Assessed or Not Applicable for it.

Diagnostic Statement Library

Hold each statement under its function, category and subcategory with an owner, a review date and the subject tags that apply.

Assessment Ratings and Evidence

Capture the rating (Yes, Yes-Risk Based, Yes-Compensating Control, Partial or No), the rationale and the supporting artifacts for every statement.

Gap Remediation Tracking

Open an action for each Partial or No rating with an owner and due date, and re-assess when the tier or the risk picture changes.

Extend: Third-Party Controls

Link the Extend statements to vendor assessments in Third Party Risk Management so supplier findings feed the Profile.

Regulatory Mapping and Board Reporting

Show results by function and category and trace each statement to the regulations it is mapped to, for examiners and the board.

Common framework mappings

NIST CSF 2.0 · NIST 800-53 Rev.5 · NYDFS 23 NYCRR 500 · EU DORA · EBA GL/2019/04 · MAS TRM 2021 · CISA CPG · FFIEC IT Handbook · MITRE ATT&CK · CIS Controls v8.1

Official resources

CRI Profile Overview and Downloads (v2.2)

Cyber Risk Institute page for the current CRI Profile v2.2: the download, mappings catalog, Guidebook, User Guide and Impact Questionnaire.

cyberriskinstitute.org/cri-profile-overview

NIST Cybersecurity Framework Overview

Outlines the structure and components of the NIST Cybersecurity Framework for organizations.

nist.gov/cyberframework

CRI Profile FAQ

CRI's answers on why the Profile was built, how it differs from NIST CSF, who can use it, voluntary use and license terms.

cyberriskinstitute.org/profile-faq

CRI Profile v2.2 Release Announcement

CRI press release of April 30, 2026: 13 new and three updated mappings, 40 in total, with no change to the core diagnostic statements.

cyberriskinstitute.org/cyber-risk-institute-releases-cri-profile-v2-2-and-new-ai-implementation-resources-to-support-financial-sector-risk-management

Frequently asked questions

Is the CRI Profile mandatory?

No. CRI says use of the Profile is entirely voluntary and that no regulator mandates it. When the FFIEC retired its Cybersecurity Assessment Tool on August 31, 2025, it said institutions may also consider the CRI Cyber Profile, and it stated that it does not endorse any particular tool.

What changed in version 2.2 of the CRI Profile?

Version 2.2, released on April 30, 2026, added 13 new mappings and updated three existing ones, for 40 mappings in total. CRI states that it did not change the core diagnostic statements, so institutions can keep their existing assessments while adopting the new mappings.

How many diagnostic statements apply to my institution?

It depends on your Impact Tier, which a nine-question questionnaire sets from systemic impact rather than asset size. Under version 2.0, 318 statements apply to Tier 1, 311 to Tier 2, 282 to Tier 3 and 208 to Tier 4 (CRI Profile Fact Sheet). Tier 1 means national or super-national impact and Tier 4 means localized impact.

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.

What is the Extend function?

Extend is the seventh function in the CRI Profile, added in version 2.0 for third-party lifecycle management. NIST CSF 2.0 places supply chain risk management inside its Govern function, and CRI gave it its own function so that financial institutions can find third-party risk issues more easily (CRI Profile Fact Sheet).

How does the CRI Profile relate to NIST CSF 2.0?

Version 2.0 and later are fully aligned to NIST CSF 2.0 and include a direct mapping to it. The Profile adds the Extend function, diagnostic statements that elaborate each subcategory and mappings to sector regulations. A "NIST CSF v2 Mapping" column shows every place where the Profile departs from NIST (CRI Profile Fact Sheet).

License included / downloadable: Yes The Cyber Risk Institute offers the Profile as a free download after a short registration, under a Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 license. Commercial use goes through CRI's Affiliate and Innovator programs, and the Maturity Model is open only to CRI members, Innovators and Affiliates. SmartSuite does not include the Profile workbook in the platform.

Full framework page and mappings: smartsuite.com/frameworks/cri-profile-cyber-risk-institute-profile

Updated Oct 15, 2026 · © 2026 SmartSuite Inc. All rights reserved.