

CRI Profile (Cyber Risk Institute)

CRI Profile is a cybersecurity risk management framework helping financial institutions assess, manage, and report cyber risks to regulators.



What it is

The CRI Profile—Cyber Risk Institute Profile is a cybersecurity risk management framework that enables financial institutions to assess, manage, and communicate cyber risks in alignment with regulatory expectations. This framework provides structured guidance for identifying cyber threats, evaluating controls, and supporting the implementation of effective security strategies.

Developed and maintained by the Cyber Risk Institute in collaboration with leading financial services organizations and regulators, the CRI Profile aligns with frameworks such as the NIST Cybersecurity Framework and the FFIEC Cyber Assessment Tool. It is tailored for use by banks, insurance companies, and other financial sector entities to address critical areas including cybersecurity controls, risk management, data protection, and operational resilience.

At a glance

<div>PUBLISHER</div> Cyber Risk Institute	<div>TYPE</div> Guidance	<div>VERSION</div> CRI Profile v2.1
<div>EFFECTIVE</div> May 2022	<div>DOMAIN</div> Risk Management	<div>FAMILY</div> Other
<div>REGION</div> United States	<div>INDUSTRY</div> Financial Services	<div>ADOPTION MODEL</div> Risk Management
<div>IMPLEMENTATION COMPLEXITY</div> High		

Source: <https://cyberriskinstitute.org/the-profile/>

Why it matters

- **Improve cybersecurity governance** Establish structured accountability for managing cyber risk across the organization's cybersecurity program and operations.
- **Enhance regulatory alignment** Support compliance with financial sector cybersecurity requirements by mapping CRI Profile controls to applicable regulatory obligations.
- **Promote operational resilience** Strengthen the institution's ability to anticipate, withstand, and recover from cyber incidents affecting critical financial operations.
- **Strengthen third-party risk management** Assess preparedness, identify gaps in vendor and partner controls, and manage third-party cyber risks within the financial ecosystem.

How SmartSuite supports CRI Profile

CRI Control Profile Management

Organize CRI Profile controls aligned to NIST CSF and financial services requirements.

Control Mapping and Regulatory Alignment

Map controls to FFIEC, NYDFS, NIST, and other regulatory frameworks.

Risk Assessment and Remediation Tracking

Track risk assessments, control evaluations, and remediation activities.

Evidence Collection and Continuous Monitoring

Capture supporting evidence and monitor control effectiveness over time.

Third-Party and Vendor Risk Integration

Link CRI controls to vendor assessments and third-party risk management.

Compliance Posture and Audit Readiness Reporting

Provide dashboards showing compliance posture, gaps, and audit readiness.

Common framework mappings

COBIT 2019

FFIEC CAT

ISO 27001:2022

ISO 27002:2022

NIST CSF 2.0

NIST 800-53 Rev.5

NYDFS 23 NYCRR 500

PCI DSS 4.0.1

SOC 2

Official resources

Cyber Risk Institute Profile

Defines the structure and content of the CRI Profile framework for financial institutions.

cyberriskinstitute.org/the-profile

NIST Cybersecurity Framework Overview

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

nist.gov/cyberframework

FFIEC Cybersecurity Assessment Tool

Provides regulatory assessment criteria compatible with the CRI Profile for risk evaluation.

ffiec.gov/cyberassessmenttool.htm

Frequently asked questions

What is the CRI Profile used for?

The CRI Profile is a cybersecurity risk management framework designed to help financial institutions assess, manage, and communicate cyber risks in alignment with regulatory expectations. It provides a structured approach to evaluating cybersecurity controls, conducting risk assessments, and supporting compliance with industry regulations.

Is the CRI Profile mandatory or certifiable?

The CRI Profile is not a mandatory or certifiable framework. Instead, it serves as a voluntary tool to assist financial institutions in aligning their cybersecurity programs with regulatory and supervisory expectations defined by agencies such as the FFIEC and NIST.

Who should use the CRI Profile?

The CRI Profile is tailored for banks, insurance companies, and other organizations in the financial services sector. It is intended for use by security leaders, compliance teams, risk managers, and IT auditors working to address cybersecurity, operational resilience, and regulatory requirements.

What key concepts and artifacts are required by the CRI Profile?

Key concepts of the CRI Profile include control families, governance domains, a maturity model, and the mapping of internal controls to risk management processes. Required artifacts typically include documented risk assessments, evidence of control effectiveness, and records supporting compliance with regulatory requirements.

How do organizations implement the CRI Profile?

Organizations implement the CRI Profile by mapping their existing controls to the framework, conducting risk assessments based on those mappings, and integrating findings into their risk governance and compliance programs. This process includes prioritizing remediation efforts, deploying monitoring controls, and maintaining documentation for regulatory review.

How does the CRI Profile relate to other cybersecurity frameworks?

The CRI Profile aligns closely with other well-established cybersecurity frameworks like the NIST Cybersecurity Framework and the FFIEC Cyber Assessment Tool. It builds upon their requirements and enables organizations to demonstrate compliance with multiple regulatory standards through a unified approach.

What are the ongoing compliance requirements for the CRI Profile?

To maintain compliance with the CRI Profile, organizations must regularly update risk assessments, monitor control effectiveness, manage third-party risks, and track remediation actions. Continuous improvement and readiness for regulatory examinations are core ongoing requirements.

How would SmartSuite support CRI Profile?

SmartSuite can help organizations operationalize the CRI Profile by providing centralized risk tracking, control management, and evidence collection for compliance purposes. The platform streamlines audit readiness with customizable documentation workflows and dashboards, supports automated remediation tracking, and enables robust reporting to demonstrate alignment and continuous improvement.

License included / downloadable: Yes The CRI Profile framework is publicly available through the Cyber Risk Institute.

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