March 2023

# The Cyber Risk Institute Profile:

*A Financial Sector Use Case of the NIST Cybersecurity Framework*

# The Cyber Risk Institute Profile:

*A Financial Sector Use Case of the NIST Cybersecurity Framework*

## Table of Contents

## I. Introduction

*The Development of the CRI Profile*

Financial institutions, like many other critical infrastructure companies, have long been subject to multiple regulatory requirements and unaligned frameworks across various agencies and countries. As the cybersecurity landscape has evolved over time, financial sector regulations have increased as well, requiring financial institutions to both adapt to threats and effectively satisfy compliance requirements. In 2016, the financial sector conducted a survey of Chief Information Security Officers for financial institutions and found that up to 40 percent of their time was spent on compliance-related activities rather than on frontline cybersecurity.

The Financial Services Sector Coordinating Council (FSSCC) began with a mapping exercise of regulatory expectations to the NIST Cybersecurity Framework (CSF), which showed that most cybersecurity regulatory expectations aligned with the cyber risk management outcomes expressed in the CSF's functions, categories, and subcategories. This mapping indicated largely similar expectations but with differences in how those expectations were phrased. This mapping exercise also highlighted that financial sector regulators were acutely focused on two additional areas—sound cybersecurity governance and supply chain risk management. *Figure 1* below depicts 2,300 supervisory

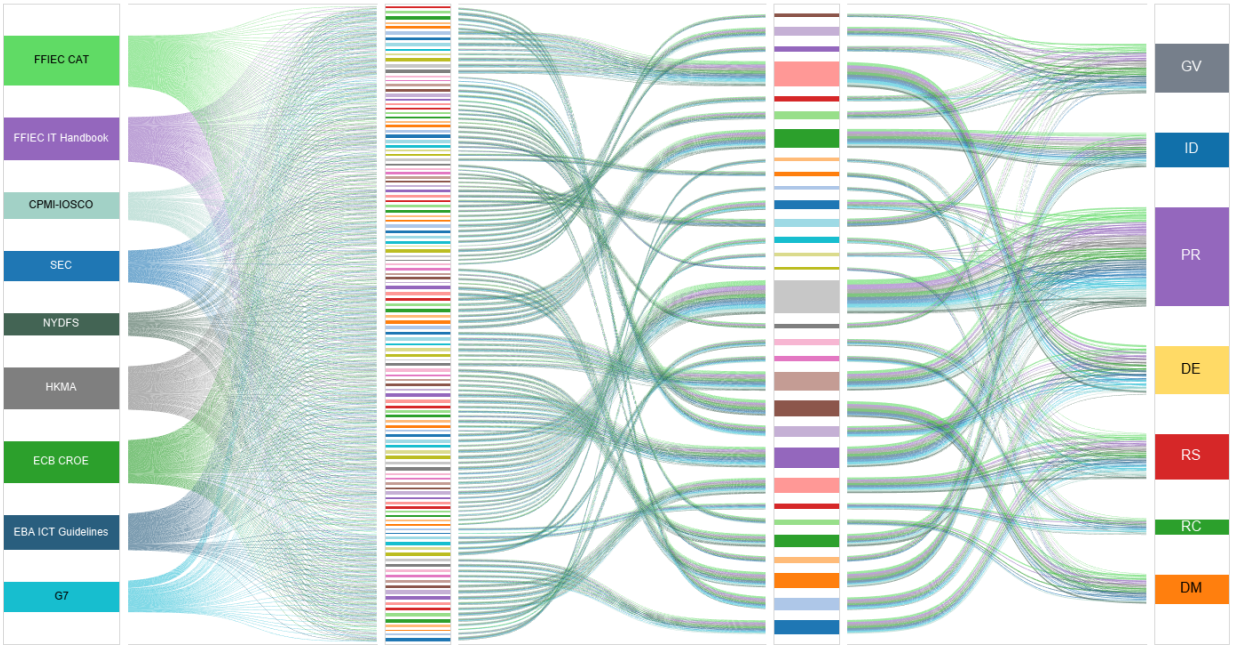


**Figure 1 —** *Topical Overlap but Differences in Phrasing*

issuances related to cybersecurity in the financial sector and how they align to the NIST CSF and additional governance and supply chain risk management functions. Governance issuances are indicated by "GV" and supply chain/dependency management issuances are indicated by "DM" in the graphic below.

As a result, the FSSCC initiated a multi-year initiative to develop a framework that would assist both industry and regulators during the compliance process. Through the course of multiple working sessions with over 300 individual experts from over 150 financial institutions, the FSSCC developed and published the Financial Sector Cyber Profile v1.0 in 2018 based on the NIST CSF. In August 2019, the financial sector regulators, through the Federal Financial Institutions Examination Council (FFIEC) issued a press release pointing to the Profile as a tool that institutions may choose from to help align "with industry standards and best practices to assess their cybersecurity preparedness."[1]

[1]FFIEC, *"FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness,"* (Washington, D.C.: August 28, 2019). https://www.ffiec.gov/press/pr082819.htm

## II. CRI Profile Components

*Description of the CRI Profile*

The Profile is based on the National Institute for Standards and Technology's (NIST) Cybersecurity Framework (CSF), but extended to include additional functions, control principles (called diagnostic statements), and regulatory references specific to the financial sector. It is from the CSF, in fact, that the Profile derives its name—it is a "Framework Profile" based on guidance provided in the CSF. Like the CSF, the Profile is a framework for understanding cyber risk, and it has also been extended to be both a self-assessment tool and a means for institutions to communicate internally and externally.

The CRI Profile consists of three primary components: (1) the Profile core that leverages the NIST CSF; (2) diagnostic statements and responses that provide a greater level of

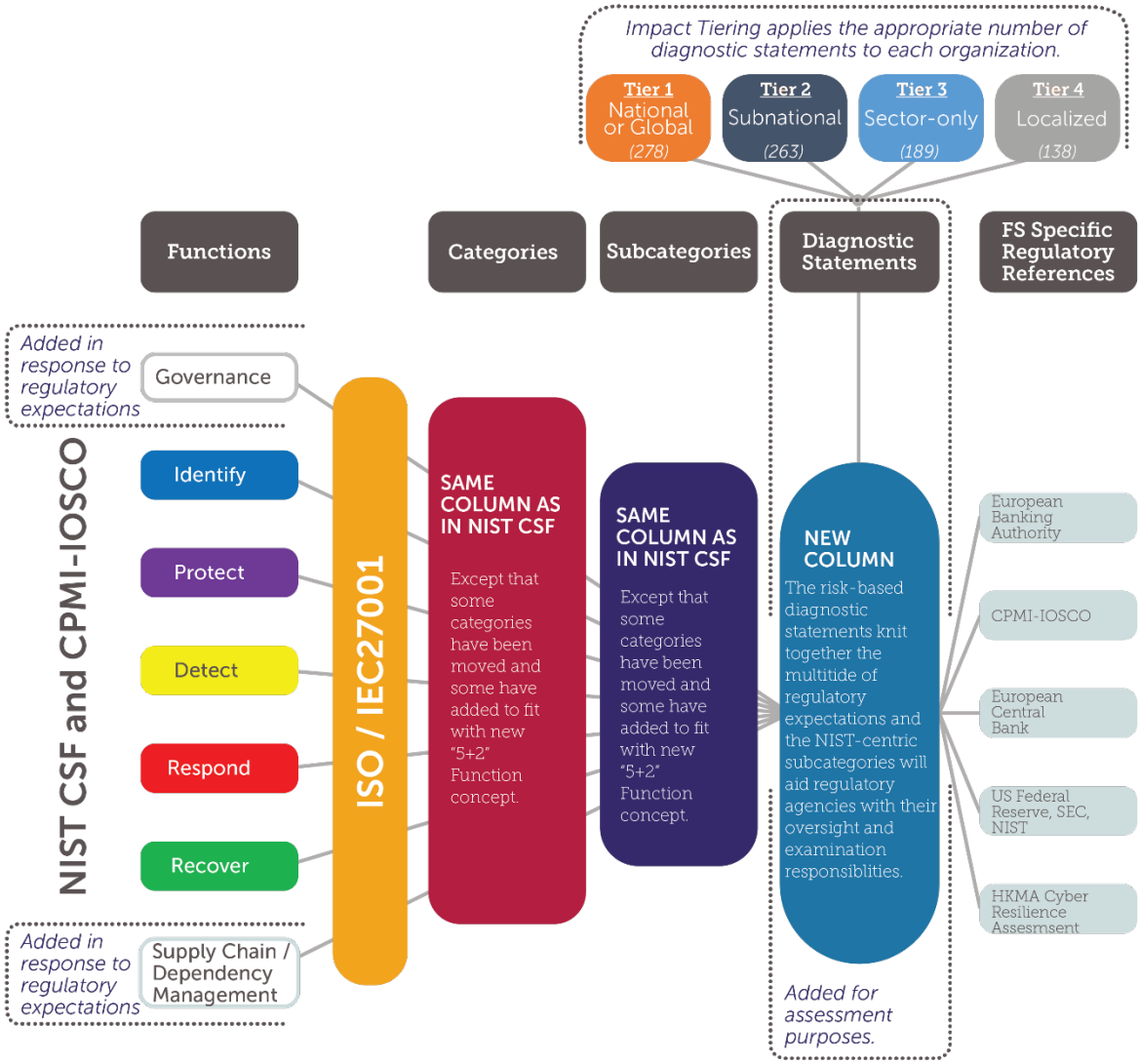


**Figure 2 —** Overview of the CRI Profile

granularity and an ability to self-assess compliance; and (3) a tiering questionnaire that allows for scalability across financial institution risk impact levels when implementing the CRI Profile. See Figure 2 for an overview of the CRI Profile's architecture.

The CRI Profile leverages the five functions in the NIST CSF (Identify, Protect, Detect, Respond, and Recover) but includes two additional functions: "Governance" and "Supply Chain/Dependency Management." The Governance function was added to address growing concerns related to cyber risk management and organizational alignment. This function includes categories from the NIST CSF's "Identify" function, such as business environment and risk management, as well as additional oversight and assurance activities cited in regulatory issuances. Additionally, the CRI Profile includes a "Supply Chain/Dependency Management" function to address growing concerns related to third-party risks faced by financial institutions and industry more broadly. This function includes categories from the NIST CSF's "Identify" function, such as supply chain and business environment activities. By elevating these control activities to a function, organizations are better able to communicate the critical elements of cyber risk management today.

The CRI Profile then extends these functions to categories and subcategories, each of which is associated with at least one Diagnostic Statement. Institutions use Diagnostic Statements to assess their own cyber risk management program. Institutions then note the outcome of their assessment by selecting one of eight potential Diagnostic Statement responses (Yes, No, Partial, Not Applicable, Not Tested, Yes-Risk Based, Yes-Compensating Controls Used, I Don't Know). An institution then collects and maintains documentation and other evidence to support its assessment and response.

*Impact Tiering Questionnaire*

Moreover, the Profile includes an "impact" questionnaire that allows an institution to adjust the number of controls it implements depending on its risk posture, in recognition that each organization has a different risk environment and tolerance. The impact questionnaire is based on global methodologies, such as the Basel Committee's determinations for globally systemic and important banks (G-SIBs), transaction volume, and interconnectedness.

Through the impact tiering questionnaire, the Profile segments the financial services sector into four tiers of criticality. Each tier corresponds with the impact that an institution would have on the global, national, sector, or local market if substantially affected by a cybersecurity event. Specifically, Tier 1 assumes the gross cyber risk exposure of an institution or service would have the most potential adverse impact to the overall stability of the global economy. Tier 2 assumes a substantial adverse impact to the financial services sector and subnational regional economy. Tier 3 includes institutions that have a high degree of interconnectedness, with certain institutions acting as key nodes within and for the sector. Tier 4 includes institutions that have a limited impact on the overall financial services sector and national economy.

As a result, the Profile is usable for financial organizations of any size and can serve as a model for tailoring by other sectors. In addition to aligning cybersecurity regulatory expectations and authorities, the Profile also provides a flexible structure to absorb future cyber, as well as operational resilience, supervisory expectations within its organization, vocabulary, and taxonomy.

*Reference Libraries, Mappings, and Guidance*

The CRI Profile includes two reference libraries—Financial Sector References and the Informative References—that act as guideposts to assist institutions in understanding the origins of the concepts (and, at times, the language) reflected in each Diagnostic Statement. In most cases, the Diagnostic Statements merge state and federal financial services sector regulation, guidance, supervisory documentation and issuances, as well as international standards and common best practices. The reference libraries are included to assist the institution in developing a roadmap to address gaps and shortcomings. Many of the references have specific instructions or detail correct security approaches and best practices.

The CRI Profile also includes numerous mappings to regulations, guidance, and standards, including the FFIEC's Cybersecurity Assessment Tool (CAT), the New York State Department of Financial Services Part 500 cybersecurity regulation, and the European Central Bank's Cyber resilience oversight expectations for financial markets. CRI endeavors to work with the regulatory community to obtain and incorporate feedback into the mappings.

Additionally, CRI developed the CRI Profile Workbook that provides specific guidance and examples of effective evidence for organizations to use during examinations. Like the CRI Profile, the Workbook is available for free on CRI's website.[2]

*Cloud Extension*

As more financial institutions move to the cloud, financial regulators globally have become increasingly focused on ensuring firms use sound risk management practices during cloud implementation. To help address challenges financial institutions and cloud service providers (CSPs) were facing, CRI, the Cloud Security Alliance (CSA), and the Bank Policy Institute-BITS developed the CRI Cloud Profile to map to CSA's Cloud Control Matrix, identify contractual responsibilities by diagnostic statement, and provide implementation guidance.

In March 2023, CRI, CSA, and the Bank Policy Institute-BITS published the Cloud Profile, which represents the collaboration of over 50 financial institutions and major cloud service providers (CSPs). The Cloud Profile provides guidance to financial institutions and CSPs on commonly understood responsibilities related to cloud deployment across software-as-a-service, platform-as-a-service, and infrastructure-as-a-service delivery models. This guidance is designed to enable financial institutions and CSPs to come to contractual

[2] https://cyberriskinstitute.org/the-profile

understanding more easily and should also facilitate more streamlined and secure processes for deploying cloud services.

*Moving the Profile to the Cyber Risk Institute*

The FSSCC, trade associations, financial institutions, and other Profile development stakeholders recognized that future maintenance of the Profile was essential. To assure the Profile's continued iteration and success, they established CRI as a separate not-for-profit organization to maintain and update the Profile. CRI was originally a separate division within the Bank Policy Institute but is now its own independent legal entity focused on standards development and regulatory harmonization and convergence efforts.

CRI membership consists of nearly 50 financial institutions and trade associations representing the broad diversity of the financial sector—from global institutions to community banks to cryptocurrency exchanges. CRI's mission is to provide a flexible framework—the CRI Profile—based on leading practices to help the financial sector better manage cyber risk.

## III. Private Sector Adoption of the CRI Profile

*Financial Sector Adoption*

NIST stated that the CSF was intended to be a "*living document and will continue to be updated and improved as industry provides feedback on implementation."*[3] The financial sector has been ahead of the curve in developing a NIST CSF-based Profile as an industry-specific assessment standard and risk communication tool. The NIST CSF continues to be the framework through which many financial services firms around the world are viewing and managing their cybersecurity risks. CRI currently has nearly 50 members, which include institutions of all sizes, who endeavor to use the Profile internally and externally. Additionally, one of CRI's key partners—the American Bankers Association—manages Profile peer groups, which collectively have over 300 participants who regularly meet to discuss Profile implementation.

With respect to the financial services industry, the CRI Profile has been designed for use by all financial institutions, financial services companies, financial firms, and their third-party providers. A broad cross-section of the financial services industry—banking, insurance, asset management, market utilities, broker-dealers—designed it to scale across institutions of varying complexity, interconnectedness, and criticality.

To facilitate adoption, the CRI Profile is available for free on its website. Financial institutions can use the Profile as the baseline cyber program assessment, and extend the functionality to evaluate partners, vendors, and third-party service providers. Like a self-assessment, a financial institution could evaluate partners, vendors, and service providers with the four Impact Tiers based upon the third parties' criticality and interconnectivity. The financial institution could then request the third party to provide evidence against the corresponding set of Diagnostic Statements identified by their Impact Tier.

*Adoption by Other Sectors*

While the Profile was developed by and for the financial services sector, it is a model that can be used in other sectors. Because the Profile is organized around the NIST CSF, organizations can flexibly address the needs of industries beyond financial services. Indeed, the Business Software Alliance used the Profile architecture to construct its *"BSA Framework for Secure Software: A New Approach to Securing the Software Lifecycle,"* a framework to help stakeholders of the software industry to evaluate the security of specific software products and services.

[3]National Institute for Standards and Technology, *Cybersecurity Framework version 1.1,* (Washington, D.C. April 16, 2018).

## IV. Benefits to the Profile Approach

The numerous and substantial benefits to the financial services sector are:

- Focuses senior executive and boardroom review of cybersecurity risks and budgeting;
- Brings plain language to benchmarking, risk management, audit, and in-house education;
- Offers compliance efficiencies that grow with a financial institution's complexity;
- Aids prioritization and focused use of resources;
- Creates a common vocabulary that eases collaboration with other financial institutions, third parties, and innovative non-bank financial companies;
- Supports tailored supervision, examinations, and collaboration among state, federal, and international supervisors;
- Enhances understanding of systemic risk within the sector, across sectors, and among institutions and third parties;
- Creates a common baseline security threshold; and
- Improves data collection and comparison.

*Benefits to Financial Institutions*

For C-Suite and board directors, cybersecurity is a top concern and supervisors expect institutions to track their progress in mitigating identified security gaps. By using the Profile over several cycles, financial institutions can benchmark their programs with the Profile's recommended practices, identify gaps, articulate those gaps to the C-Suite and board directors in plain language, discuss appropriate resourcing for mitigation, and track the advancement in mitigation efforts over time.

The Profile also reduces the time a financial institution needs to complete a comprehensive assessment by offering a tailored set of statements used for assessment purposes – the Diagnostic Statements – reflecting the institution's risk to the broader economy.

*Benefits to the Regulatory Community*

For the regulatory community, the benefits also are numerous and substantial. With the Profile, state, federal, and global supervisors can:

- Tailor examinations to institutional complexity and conduct "deeper dives" in those areas of greater importance;
- Better discern the sector's systemic risk by comparing answers across institutions using common terms and concepts;
- Understand an institution's baseline security status quickly, affording additional time for specialization, testing, and validation;
- Broaden the ability to take collective supervisory action to address identified global, national, sector, and institution risks;

- Improve data analysis and data comparisons from other agencies and jurisdictions; and
- Enhance supervisors' visibility into non-sector and third-party risks.

The organization, vocabulary, and taxonomy of the Profile offers a credible method of cybersecurity risk management and a basis for conducting supervisory exams. Supervisors may allow financial institutions to use the evidence in their Profile self-assessment exercise for supervisory reporting and analysis. This consistency will allow supervisors to evaluate and compare peer institutions and clearly identify gaps for remediation. This approach is more efficient for the institution and supervisor and provides consistency for an institution in communicating its program both internally and externally.

The use of the Profile's approach does not limit what a supervisor can review or require. Rather, it provides an examination approach allowing financial institutions to confidently produce baseline evidence for review and more quickly respond to iterative and follow-up questions from the supervisor. This shared approach would produce a more efficient and consistent examination process for supervisors and financial institutions.

## V. Updates to the CRI Profile

CRI's membership determines the regulatory provisions and industry standards that will be incorporated into the Profile. CRI plans to issue new, full revisions of the Profile with major updates every 2-to-3-years similar to those cycles used by other standards bodies, such as NIST and ISO. In addition, CRI plans to issue more minor updates, such as updates to the informative references or regulatory mappings, on a more frequent or yearly basis.

CRI has demonstrated its commitment to this regular update cycle by publishing:

- CRI Profile v1.1 in 2020
- CRI Profile v1.2 in 2021
- CRI Profile Workbook for v1.2 in 2021
- CRI Cloud Profile Extension in 2022
- CRI Profile v1.2.1 in 2023

CRI intends to publish its most significant update—Profile v2.0—in mid- to late-2023, which will include additional coverage of cybersecurity, technology, business resilience, and third-party risk related topics.

## VI. Stakeholder Recognition

The CRI Profile is unique from other standards and frameworks in that it incorporates feedback provided by regulators. CRI has received recognition from regulators from around the world, including:

U.S. Department of the Treasury:

- "In many cases, financial institutions may follow or repurpose as, according to their needs, sector-agnostic approaches such as those outlined by NIST (e.g., NIST SP 500-291 Cloud Computing Standards Roadmap or SP 500-332 Cloud Federation Reference Architecture) or financial sector-specific approaches, like the **Cyber Risk Institute's "Cloud Profile**….Industry and financial authority toolkits and best practices for financial institutions continue to evolve. For example, the Cyber Risk Institute's cloud profile provides financial institutions with a framework to evaluate cybersecurity risk with cloud services"[4]

- "As we [Treasury] develop our [Cloud use in the financial services] report and over the longer term as we continue to work on these issues, we will collaborate with the private sector and organizations like **Cyber Risk Institute**, FBIIC members, and our international partners, many of which are considering increasing their oversight of cloud service providers" (emphasis added). Todd Conklin, Treasury Deputy Assistant Secretary for the Office of Cybersecurity and Critical Infrastructure Protection.

- "Treasury, as Sector Risk Management Agency for the financial services sector, appreciates the inclusion of precision time resiliency into the **CRI Profile**. This collaboration on responsible use of precision time enables the sector to fully benefit from the Biden-Harris Administration's continued work on this Executive Order."[5]

Commodity Futures Trading Commission (CFTC):

- "The CFTC welcomes collaborative approaches to advance and support cyber preparedness and enhance the efficiency and effectiveness of its system safeguards oversight. To this end, the CFTC welcomes use by regulated entities of standardized tools aligned with industry standards and best practices to assess their cybersecurity preparedness. Such tools include the **[CRI] Cybersecurity Profile**, the NIST Cybersecurity Framework, the ISO Cybersecurity Standard, and the ISACA COBIT Framework, among others."[6]

---

[4]U.S. Department of the Treasury, *The Financial Services Sector's Adoption of Cloud Services* (Washington, D.C.: February 8, 2023).
[5]CRI, *New CRI Updates Reflect Profile's Ability to Adapt* (Washington, D.C.: January 25, 2023). https://cyberriskinstitute.org/new-cri-updates-reflect-profiles-ability-to-adapt/
[6]CFTC, *CFTC Encourages Standardized Approaches to Assessing Cybersecurity Preparedness, Including the FSSCC Cybersecurity Profile* (Washington, D.C.: July 16, 2020). CFTC Encourages

FFIEC *(Federal Reserve Board (FRB), Office of the Comptroller of the Currency (OCC), Consumer Financial Protection Bureau (CFPB), National Credit Union Administration (NCUA), Federal Deposit Insurance Commission (FDIC):*

- "Institutions may choose from a variety of standardized tools aligned with industry standards and best practices to assess their cybersecurity preparedness. These tools include the FFIEC Cybersecurity Assessment Tool, the National Institute of Standards and Technology Cybersecurity Framework, the **[CRI] Profile**, and the Center for Internet Security Critical Security Controls."[7]

New York State Department of Financial Services (NYDFS):

- NYDFS provided positive feedback on the mappings of its Part 500 regulation to the Profile and, in December, published a statement in support regarding Profile use by examined entities in its online FAQs:
    - "Among the widely used frameworks Covered Entities employ are the FFIEC Cyber Assessment Tool, the **CRI Profile**, and the NIST Cybersecurity Framework."[8]

Reserve Bank of New Zealand:

- The **CRI Profile** was listed as a "recommended framework for regulated entities to refer to" when building their cyber resilience by the Reserve Bank of New Zealand.[9]

International Regulatory Strategy Group (ISRG):

- The IRSG recommended that the G7 call for the adoption of the **CRI Profile** as the "accepted supervisory baseline upon which national variations can be established for supervisors."[10]

UK Finance:

- "**The Profile's** modular and scalable nature mean that it can readily incorporate additional regulatory frameworks to evolve with the changing regulatory landscape. This flexible design is why the Profile remains relevant now and will do so in the future, and why firms across the UK and mainland Europe are

Standardized Approaches to Assessing Cybersecurity Preparedness, Including the FSSCC Cybersecurity Profile | CFTC

[7]FFIEC, *"FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness,"* (Washington, D.C.: August 28, 2019). https://www.ffiec.gov/press/pr082819.htm

[8]NYDFS, *FAQ #10.* Cybersecurity Resource Center | Department of Financial Services (ny.gov)

[9]Reserve Bank of New Zealand, *Guidance on Cyber Resilience* (Washington, D.C.: April 2021). Guidance on cyber resilience (rbnz.govt.nz)

[10]International Regulatory Strategy Group, *Financial SERBICES Priorities for the UK's G7 Presidency* (London, UK: June 2021). Financial Services Priorities for the UK's G7 Presidency (irsg.co.uk)

increasingly using it as a cyber risk assessment and regulatory convergence instrument."[11]

ENISA (EU):

- The **CRI Profile** was recognized by the EU Cybersecurity Agency, ENISA, as a "Major Cybersecurity Initiative in Europe."[12]

FRB, OCC, FDIC:

- "Some of the tools that firms can choose from include the FFIEC Cybersecurity Assessment Tool, the National Institute of Standards and Technology Cybersecurity Framework (NIST), the Center for Internet Security Critical Security Controls, and the [CRI] **Profile**."[13]

World Economic Forum:

- "The FSC Profile streamlines the process of complying with varying regulatory regimes and is adapted for markets in North America, Europe and Asia-Pacific…Because the [CRI] Profile maps to financial services regulations and has the support of major US and European financial services firms,23 it will facilitate many types of partnership between FinTechs and regulated financial services firms operating in these regions. It has the potential to be scaled globally as it integrates regulations from more regions through its regular update process."[14]

International Organization of Securities Commissioners (IOSCO):

- "Of the jurisdictions that have adopted a national Cyber Security strategy, policy or framework, many also reference or expressly follow the tools and good practices in other Cyber frameworks or guidance as well. These other Cyber standards include: **[CRI] Profile**, Version 1.0.[15]

National Institute of Standards and Technology (NIST):

- "NIST has found the [CRI] Profile Version 1.0 to be 1) correct with regard to Cybersecurity Framework Version 1.2., 2) supportive of a risk-based approach to

[11]UK Finance*, A Unified Approach for Assessing Cybersecurity Risk – The Profile (London, UK:* April 2021). A unified approach for assessing cybersecurity risk - the Profile | Insights | UK Finance
[12]ENISA, *EU Cybersecurity Initiatives in the Finance Sector* (March 5, 2021). EU Cybersecurity Initiatives in the Finance Sector — ENISA (europa.eu)
[13]FRB, OCC, FDIC; *Sound Practices to Strengthen Operational Resilience* (Washington, D.C.: October 2020).
[14]World Economic Forum, *Systems of Cyber Resilience: Secure and Trusted FinTech* (Geneva, Switzerland: )
[15]OICU-IOSCO, *The Board of the International Organization of Securities Commissioners: Final Report* (June 2019).

cybersecurity, and 3) one of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to date."[16]

Securities and Exchange Commission (SEC):

- In 2019, the SEC published three notices of filings of proposed rules changes, which included references to the CRI Profile:
    - "Examples of recognized frameworks, guidelines and standards that DTC believes are adequate include the Financial Services Sector Coordinating Council Cybersecurity Profile."[17]

[16]NIST, *Letter to the Financial Services Sector Coordinating Council Chair,* (Washington, D.C.: October 18, 2018). NIST-Letter-of-Support-re-FSSCC-Financial-Services-Sector-Cybersecurity-Profile.pdf (cyberriskinstitute.org)

[17]SEC, *Self-Regulatory Organizations; The Depository Trust Company; Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity Program* (Washington, D.C.: October 24, 2019) Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity Program; *Self-Regulatory Organizations; National Securities Clearing Corporation; Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity Program* (Washington, D.C.: October 24, 2019) Notice of Filing of Proposed Rule Change to Require Confirmation of Cybersecurity Program; *Self-Regulatory Organizations; Fixed Income Clearing Corporation; Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program* (Washington, D.C.: December 9, 2019) Order Approving a Proposed Rule Change to Require Confirmation of Cybersecurity Program;