Table of Contents

I. Introduction

Background: With the increasing volume and sophistication of cyber-attacks and a projected global shortfall of three and a half million cybersecurity professionals for this year, 2021, the financial services and supervisory community continue to struggle to find an efficient approach to cybersecurity risk management that effectively counters the dynamic, evolving threat and provides adequate assurance to government supervisors.

When last surveyed in 2016, Chief Information Security Officers for financial services institutions reported that up to 40% of their time was spent on the compliance requirements of various regulatory frameworks, not cybersecurity.

The CRI Profile (previously known as the "FSSCC Profile," "Financial Services Profile," the "FSP," or "the Sector Cybersecurity Profile") is an assessment framework based on: the National Institute of Standards and Technology's "Framework for Improving Critical Infrastructure Cybersecurity" (NIST Framework or CSF), CPMI-IOSCO's "Guidance on cyber resilience for financial market structures," assessment questions based on relevant supervisory guidance and frameworks, and direct correlative mappings to ISO/IEC 27001/2 controls.

To enhance the Profile's assessment capabilities, the industry developed an "Impact Tiering" questionnaire to identify the potential market risk presented by financial institutions of differing complexity, and sizes. This "Impact Tiering" approach was encouraged by the regulatory community, and the concepts included in this approach are concepts that they now express in their policy initiatives regarding operational resilience. While the original impact tiering focused on the North American financial sector, it is easily expandable to include other international jurisdictions.

Purpose and Intent: 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. Institutions and supervisory agencies and organizations can focus on the core elements of their cyber risk management missions. With the efficiencies gained, more resources can then be applied to cybersecurity.

II. Which Types of Institutions Is the Profile Designed For?

While the Profile was developed by the financial services sector, it is a model that can be (and has been) used in other sectors. The Profile is organized around the seven Functions of (1) Governance, (2) Identify, (3) Protect, (4) Detect, (5) Respond, (6) Recover, and (7) Supply/Dependency Management and extended with Diagnostic Statements to connect these concepts with existing compliance requirements and informative references, such as the ISO 27000 series controls, which makes it flexible to address the needs of industries beyond the 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.

With respect to the financial services industry, the 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. Regulatory issuances and best practices from across the sector and around the globe are incorporated and continue to be integrated through the work of CRI.

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. These "Impact Tiers" are as follows:

> ***Tier 1: National/Super-National Impact***. This tier includes institutions that are designated *most critical* by one or more U.S. or North American regulatory agencies and/or bodies (e.g., GSIB designation; Executive Order 13636, Section 9 designation). This category assumes the gross cyber risk exposure of an institution or service categorized as Tier 1 would have the most potential adverse impact to the overall stability of the global economy.
>
> ***Tier 2: Subnational Impact***. This tier includes institutions that provide mission critical services for millions of customer accounts. This category assumes the gross cyber risk exposure of an institution or service would have the potential for a substantial adverse impact to the financial services sector and subnational regional economy but does not rise to the level of Tier 1.
>
> ***Tier 3: Sector Impact***. This tier includes institutions that have a high degree of interconnectedness, with certain institutions acting as key nodes within and for the sector. The nature of the services that these institutions provide to the sector plays a significant role in determining their criticality.
>
> ***Tier 4: Localized Impact.*** This tier includes institutions that have a limited impact on the overall financial services sector and national economy. Typical characteristics include: (a) institutions with a local presence and less than 1 million customers (e.g., community banks, state banks) and (b) providers of low criticality services in relation to the entire sector.

Upon determining an institution's Impact Tier, the Profile is customized to meet the institution's likely cybersecurity risk. The user is then prompted to answer a set of self-assessment questions—the Diagnostic Statements—coded by Function, Category, Subcategory, and associated numbering with the CPMI-IOSCO and NIST Cybersecurity Framework.

Financial institutions can use the Profile as the baseline examination assessment, and extend the functionality to evaluate partners, vendors, and third-party service providers.

It is important to note that these tiers are provided as guidance. An organization can include Diagnostic Statements associated with a different tier than the one with which they identify. Potential reasons for lower tiered organizations to include additional Diagnostic Statements corresponding with other tier levels may include business interests, risk appetite, or third-party or regulator expectations. Similarly, while an institution may categorize itself at a certain tier, an outside organization using the Profile to evaluate the institution's cybersecurity posture may categorize the institution into a different Impact Tier.

III. 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

Boardroom Engagement to Advance Investment: 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.

Efficiencies: The Profile promises to reduce 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.

- **73% Reduction for Community Institution Assessment Questions.** For the least complex and interconnected institutions, it is expected that they will answer a total of 146 questions (9 tiering questions + 137 Diagnostic Statement questions). Compared

with another widely-used assessment tool's 533 questions, the Profile represents ***a 73% reduction*** in questions.

- **49% Reduction in Assessment Questions for the Largest Institutions.** For the most complex and interconnected institutions, the reduction also is significant. With the Profile, it is expected that such institutions will answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions) as compared to the other widely-used assessment's 533, the Profile represents ***a 49% reduction*** in questions.

Benefits to Regulatory Community

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

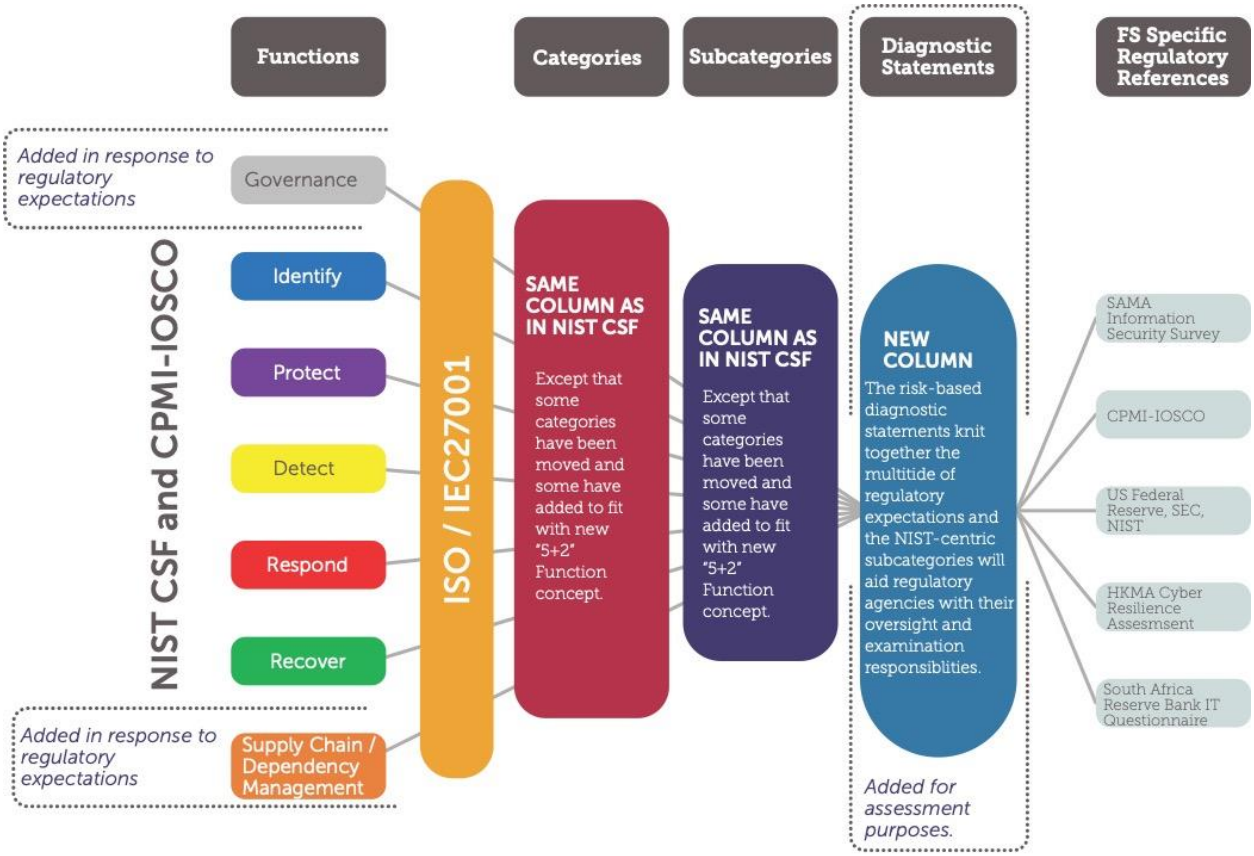
- Tailor examinations to institutional complexity and conduct "deeper dives" in those areas of greater importance;
- Better discern the sector's systemic risk by comparing answers across institutions using common terms and concepts;
- Understand an institution's baseline security status quickly, affording 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.

IV. Core Profile Components

The Core Profile Components consist of the following:

- ***Functions*** (found in Column A in the "v1.2 Diagnostic Statements" tab);
- ***Categories*** (found in Column B in the "v1.2 Diagnostic Statements" tab);
- ***Subcategories*** (found in Column C in the "v1.2 Diagnostic Statements" tab);
- ***Diagnostic Statements*** (found in Column F in the "v1.2 Diagnostic Statements" tab);
- ***Potential Responses*** for each Impact Tier's Diagnostic Statements (for Impact Tier 1, 2, 3, and 4 firms, responses can be found by clicking on cells in Columns G, H, I, and J, respectively, in the "v1.2 Diagnostic Statements" tab);
- ***Financial Sector Reference*** - i.e., where in existing regulations, guidance or other supervisory documents the concept is applied to the Financial Sector (found in Column K in the "v1.2 Diagnostic Statements" tab); and
- ***Informative References*** - i.e., where the corresponding concept is expressed in international standards and best practices (found in Column L in the "v1.2 Diagnostic Statements" tab.

See figure below.



<u>There are seven overarching functions:</u> (1) Governance, (2) Identify, (3) Detect, (4) Protect, (5) Respond, (6) Recover, and (7) Supply Chain/Dependency Management. These are adapted from the NIST Framework and CPMI-IOSCO to more closely align with the financial services sector approach to cybersecurity.

Functions are subdivided into more specific concept categories (Categories).

Categories are sub-divided into subcategories (Subcategories), which are designed to reflect a particular element of an effective cyber risk management program.

Each Subcategory 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:

1) **Yes**: An institution would select this response if it can confidently answer Yes;
2) **No:** An institution would select this response if it has not fulfilled the Diagnostic Statement;

3) **Partial:** An institution would select this response if it has not fully met the Diagnostic Statement, but it is currently working through an action plan to achieve a Yes outcome;
4) **Not Applicable:** An institution might select this response if, after evaluating its business and security program, the Diagnostic Statement is not applicable even though it was suggested by its Impact Tier;
5) **Not Tested:** An institution might select this response if it has yet to test controls associated with that specific Diagnostic Statement;
6) **Yes-Risk Based:** An institution might select this response if the Diagnostic Statement, in using supervisory language, requires a more nuanced, risk-based answer and explanation than the Diagnostic Statement otherwise suggests;
7) **Yes-Compensating Controls Used:** An institution might select this response if it meets the intent of the Diagnostic Statement by using compensating controls; and
8) **I don't know:** An individual assessment user might select this response as a note to check with other relevant stakeholders within the institution to determine the most accurate response.

An institution would then collect and maintain documentation and other evidence to support its assessment and response.

Impact Tiers and the Impact Tier Questionnaire are a scaling device to customize the Profile based on an individual institution's risk and activities. Completing the questionnaire results in a determination of which of the four tiers of impact are most reflective of the institution's impact: National/Super-National, Subnational, Sectoral, or Localized. These are the Impact Tiers. The institution would then answer a set of Diagnostic Statements corresponding to its Impact Tier.

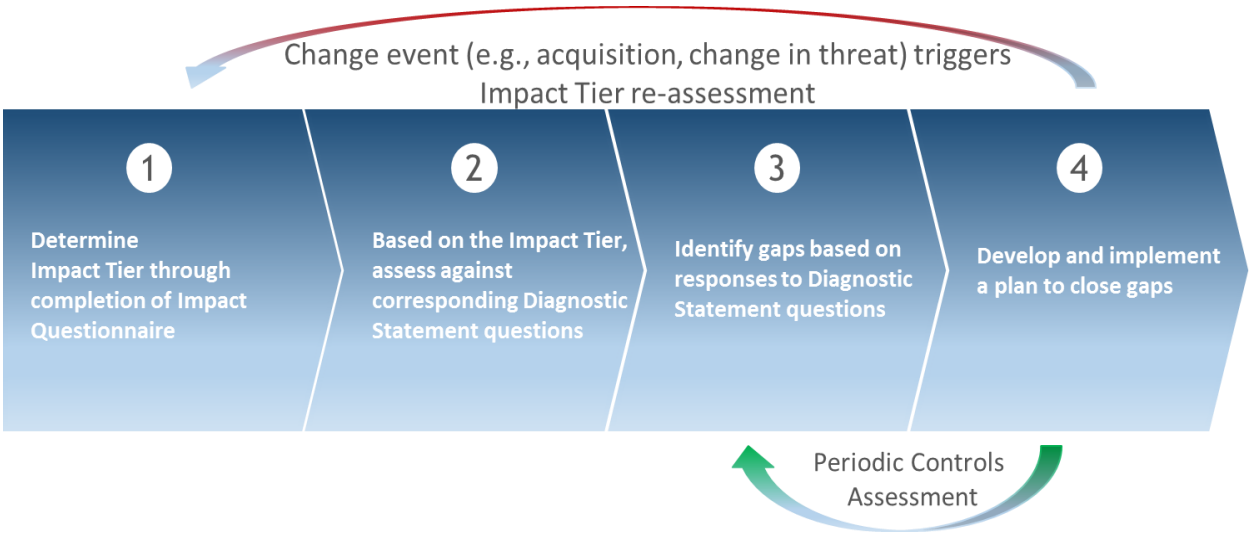
These tiers are for guidance purposes only. Subcategories and Diagnostic Statements not associated with a particular tier may be included by a supervisor or other institution that is using the Profile to evaluate cyber risk management programs.

The two reference libraries—Financial Sector References and the Informative References—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.

V. How to Use the Profile

The Profile may be used in multiple ways, from self-assessment and third-party risk management, to providing a common supervisory engagement approach among state, federal, and international regulatory bodies.

Cybersecurity Self-Assessment in Four Easy and Repeatable Steps: The Profile may assist institutions in assessing their cybersecurity risk management governance, processes, capabilities, and regulatory compliance posture as expected with the various Impact Tiers to which they correspond. In understanding their posture, institutions can then develop plans to close any identified gaps. This process can be reduced to four repeatable steps as depicted and further described below.



Step 1: The institution determines its Impact Tier by completing the Impact Tiering Questionnaire. The Questionnaire consists of nine questions that identify an institution's Impact Tier:

- Tier 1: National/Super-National Impact;
- Tier 2: Subnational Impact;
- Tier 3: Sector Impact; and
- Tier 4: Localized Impact.

Step 2: Based on the Institution's Impact Tier, the institution assesses itself against the corresponding Diagnostic Statements:

- Tier 1: 277 Diagnostic Statements;
- Tier 2: 262 Diagnostic Statements;
- Tier 3: 188 Diagnostic Statements; and
- Tier 4: 137 Diagnostic Statements.

Step 3: Based on the self-assessment, the institution identifies shortcomings and gaps in its cybersecurity risk management governance, processes, capabilities, and regulatory compliance posture.

Step 4: Once gaps are identified, the institution develops and implements a plan to close gaps and address shortcomings to satisfy the cybersecurity expectations of its Impact Tier.

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.

Repeat: The institution repeats the self-assessment and gap-closing process periodically, or upon an event, which warrants a re-evaluation of their Impact Tier, such as:

- Acquisition of another entity;
- Introduction of a new business line;
- Significant growth in number of accounts, delivery of critical services, or interconnectedness;
- A significant change in a threat landscape;
- The institution believes that their Impact Tier has changed; and/or
- A regulatory or supervisory body believes that the institution's self-assessed Impact Tier is inaccurate or has changed.

Profile as Third-Party Risk Management Tool: Like 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.

Profile as a Common Supervisory Approach: 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.

VI. Governance Process on Profile Iteration

The Financial Sector Coordinating Council (FSSCC), trade associations, financial institutions, and other Profile development stakeholders recognized that future maintenance of the Profile is

essential for its ultimate success. To assure the Profile's continued iteration and success, they established the Cyber Risk Institute (CRI) as a separate not-for-profit organization (originally a separate division within the Bank Policy Institute). CRI is tasked with maintaining and evolving the Profile. For more information about CRI, please visit: https://cyberriskinstitute.org/

CRI plans to issue new, full revisions of the Profile, which would include any major updates, every 2-to-3-years similar to those cycles used by other standards bodies, such as NIST and ISO. The next such major update will most likely occur in late 2022. 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 recognizes that users may suggest potential enhancements and new cyber risk management concepts between Profile versions. As these recommendations surface, CRI will evaluate their applicability within the regulatory landscape, utility to a cyber risk management program, and the feasibility of incorporation into a Profile's next version. This process of evaluation includes a review by the CRI Board of Directors, Standards Committee, and other stakeholders, as appropriate, as was done to develop the Profile from concept to its first release in Version 1.0.

VII. Points of Contact and Adding Trade Association Support through Logo Usage

To Learn More: To learn more about the Profile, participating in future Profile iterations, or CRI, please contact Josh Magri of the Cyber Risk Institute. To participate in Profile peer groups, please contact Denyette DePierro of the American Bankers Association, who helped lead the development of the Profile.

Adding Trade Association Support: We continue to appreciate the support of trade associations across the sector and would gladly accept additional support from additional associations as they believe the work of CRI is a benefit to their members.