Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

The Financial Services Sector Cybersecurity Profile (Profile), v1.0
- An Overview and User Guide -

Table of Contents

I. Introduction

Background: With the increasing volume and sophistication of cyber attacks and a projected global shortfall of two million cybersecurity professionals by 2019, the financial services and supervisory community are struggling to find an efficient approach to cybersecurity risk management that effectively counters the dynamic, evolving threat and provides adequate assurance to government supervisors.

However, when surveyed two years ago, 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 Financial Services Sector Cybersecurity Profile (Profile or FSP) is a framework based on:

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.

Profile Structure: Starting in October 2016, the financial services industry began mapping the many financial services regulations, guidance, and supervisory expectations with the NIST Cybersecurity Framework, CPMI-IOSCO, and the ISO standards. With multiple mappings, a pattern emerged. Over 80% of the supervisory instructions had a similar focus, but used different language, or had marginally different compliance requirements. Industry began developing the Profile to reduce the compliance time needed to reconcile these differences. As the Profile evolved, its design became rooted in the NIST Cybersecurity Framework's five functions, categories, and subcategories. To more correctly reflect supervisory emphasis, the NIST-like framework was extended to include two new functions – Governance and Supply/Dependency Management. Borrowing from the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool, the Profile adopted Diagnostic Statements, which synthesize and simplify overlapping requirements from multiple supervisors.

To enhance the Profile's assessment capabilities (and with the regulatory community's encouragement), the industry developed an "Impact Tiering" questionnaire to identify the potential market risk presented by financial institutions of differing complexity, and sizes.[1]

Purpose and Intent: In addition to aligning cybersecurity regulatory expectations and authorities, the Profile also provides a flexible structure to absorb future supervisory expectations within its organization, vocabulary, and taxonomy. Institutions and supervisory agencies and organizations can focus on the core elements of their cybersecurity risk management missions. With the efficiencies gained, more resources can then be applied to cybersecurity.

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

The Profile is designed for 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 the Profile 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.

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

[1] While the original impact tiering focused on the North American financial sector, it could be expanded to include international jurisdictions.

the global, national, sector, or local market if substantially impacted by a cybersecurity event. These "Impact Tiers" are as follows:

> ***Tier 1: National/Super-National Impact*** – These institutions 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 North American economy, and potentially, the global market.
>
> ***Tier 2: Subnational Impact*** – These institutions provide mission critical services with 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*** – These institutions 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*** – These institutions 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.

Upon determining an institution's impact category, 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.

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;

- 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 the 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 diagnostic assessment questions, 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 would answer a total of 145 questions (9 tiering questions + 136 Diagnostic Statement questions). As compared to another widely-used assessment tool's 533 questions, this represents ***a 73% reduction.***
- **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 would answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions) as compared to the other widely-used assessment's 533, ***a 49% reduction***.

Additional Benefits: While increased time and focus on cybersecurity projects and activities is a substantial benefit, continued use of the Profile would bring additional benefits. Immediate benefits for financial institutions include:

- Enhanced internal and external oversight, due diligence and risk identification using consistent terms and concepts;
- More efficient third-party vendor management review and oversight;
- Greater intra-sector, cross-sector and international cybersecurity collaboration due to the common use of ISO standards, CPMI-IOSCO and the NIST Cybersecurity Framework; and
- Encouraging innovation and adoption of emerging technology, as FinTech firms and startups can more readily demonstrate adherence to financial services sector cybersecurity requirements and supervisory expectations.

Benefits to Regulatory Community

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

- 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 represented in columns A-K on Tab 3 of the companion spreadsheet consist of the core Profile components, namely:

- Functions;
- Categories;
- Subcategories;
- Diagnostic Statements;
- Response/Evidence for each impact tier;
- Financial Sector Reference (i.e., where in existing regulations, guidance or other supervisory documents the concept is applied to the Financial Sector); and
- Informative references (i.e., where the corresponding concept is expressed in international standards and best practices).

There are seven overarching functions: Governance, Identify, Detect, Protect, Respond, Recover and 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 would then note their outcome of their assessment selecting between 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;
3) ***Partial*** – An institution would select this response if it has not fully met the Diagnostic, but 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 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 particular Diagnostic;
6) ***Yes-Risk Based*** – An institution might select this response if the Diagnostic, 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 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.

Institutions would then collect and maintain documentation and other evidence to support their 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 categories of impact are most reflective of the institution's impact: 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.

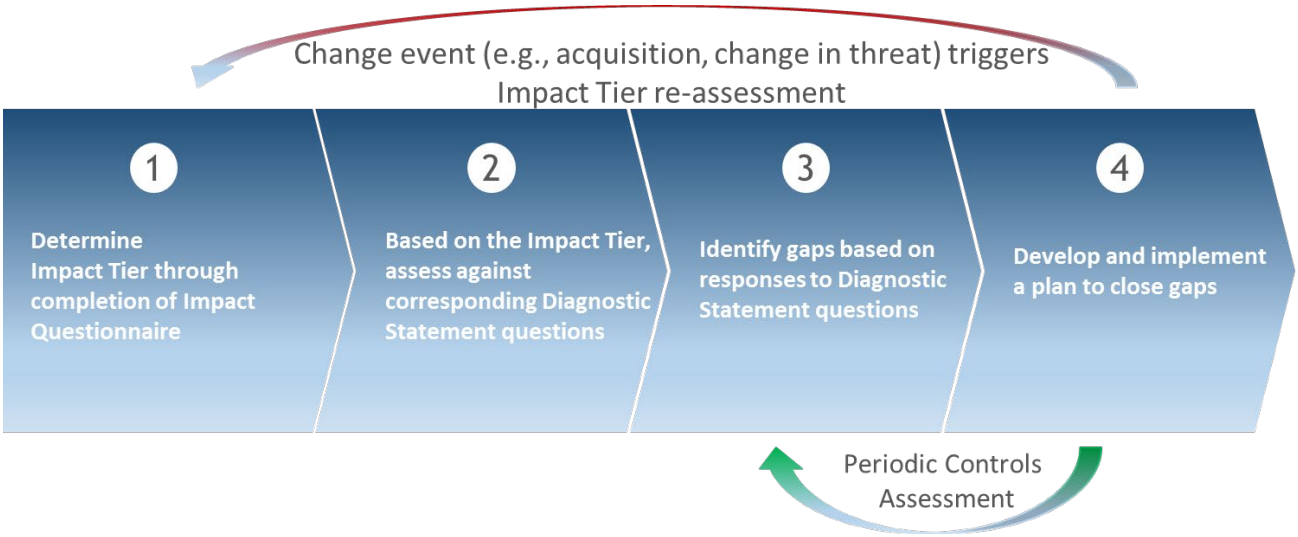
These Tiers are for guidance purposes only. Subcategories and Diagnostic Statements not associated with a particular tier may be included by a supervisor or other institution that is using the Profile to evaluate cyber risk management programs.

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 4 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 9 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 Tie, the Institution assesses itself with the corresponding Diagnostic Statement questions:

- Tier 1: 277 Diagnostic Statement questions;
- Tier 2: 262 Diagnostic Statement questions;
- Tier 3: 188 Diagnostic Statement questions; and
- Tier 4: 136 Diagnostic Statement questions.

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 an 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: Similar to 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, 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. Version 1.0 and Governance Process Going Forward

The Financial Sector Coordinating Council (FSSCC), the trade associations, financial institutions, and other Profile development stakeholders recognize that future maintenance of the Profile is essential for its ultimate success. Numerous trade associations and financial institutions involved in the Profile's development are forming a sustained coalition to manage Profile

update activities and to educate and engage jurisdictions around the world on its benefits and usage. Interested parties will continue committing resources, such as their own subject matter experts and expertise, full time personnel, and funds for external experts and advisors.

This coalition has also committed to a 2-3 year update cycle to iterate a new, full version similar to the cycles used by other standards bodies, such as the National Institute of Standards and Technology (NIST) and International Standards Organization (ISO) for a full version. The coalition has also committed to more flexible update timeframes to include additional global supervisory expectations as well as any newly issued supervisory expectations.

The coalition recognizes that users may suggest potential enhancements and new cyber risk management concepts between Profile versions. As these recommendations surface, the coalition 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 will include a review by a coalition executive committee and other stakeholders, as appropriate, as was done to develop the Profile from concept to a Version 1.0.

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

To Learn More: To learn more about the Profile initiative, please feel free to contact Profile leads: Josh Magri of Bank Policy Institute (BPI) - BITS and Denyette DePierro of the American Bankers Association.

Josh Magri
Senior Vice President, Counsel for Regulation & Developing Technology
Josh.Magri@BPI.com
Bank Policy Institute (BPI) – BITS

Denyette DePierro
Vice President & Senior Counsel
Center for Payments and Cybersecurity
ddepierr@aba.com
American Bankers Association

Adding Trade Association Support: We are collecting logos of trades that are supportive of the Profile. By allowing usage of the logo on the Profile and Profile related documents, it means that the trade association and its member institutions recognize:

> *The Financial Services Sector Cybersecurity Profile represents a comprehensive compilation of cybersecurity risk management best practices that could represent a basis for regulatory/supervisory harmonization for the financial services sector.*

Appendix A: Roadmap for Future Versions

The Roadmap for Future Versions is a standalone, companion document that will be updated between successive Profile versions. Items listed maybe reprioritized between Roadmap versions as circumstances change.

Appendix B: Frequently Asked Questions (FAQs)

1. Where can I find the Profile?

The latest, free copy of the Profile is available for download on the Financial Services Sector Coordinating Council (FSSCC) website, the NIST Cybersecurity Framework Critical Infrastructure Resources webpage: https://www.nist.gov/cyberframework/critical-infrastructure-resources, and on the websites of supporting trade associations.

2. What is the Profile? And what is it NOT?

What the Profile Is:	What the Profile is NOT:
• It is built from existing regulations, guidance, frameworks, and standards.	• It is not built from wholly original content without connection to pre-existing regulations, guidance, frameworks, and standards.
• It is unique because it efficiently weaves existing regulations and frameworks together to form a standardized taxonomy and foundational structure to organize an institution's cybersecurity risk management program.	• It is not a newly created "standard of good practice."

• It is comprehensive in scope.	• It is not exhaustive in depth. An institution should determine for itself whether there are additional state, national, or international compliance requirements that are not part of the Profile.
• It describes the fundamental, universal elements of a cyber risk management program (i.e., the "what" of the program).	• It is not intended describe how an institution should fulfill the program elements (i.e., the "how" of the program).
• Through the addition of diagnostic statements and an impact tiering construct, it functions as a scalable self-assessment that can be used by financial institutions and third-parties of differing scope, size, and complexity.	• It does not address in full the unique requirements of all institutions. It is often referred to as the 80% solution leaving room for further institution and supervisory tailoring to individual business and regulatory requirements.
• It provides a sound and informed risk management roadmap.	• It does not supersede regulatory authority, nor is it intended to replace reasonable business judgement.

3. Why was the Profile developed?

When surveyed two years ago, 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.[2]

For financial institutions, if the Profile approach is implemented, accepted by supervisory agencies for use, and maintained by industry, the benefits would be tremendous. Focusing cybersecurity experts' time on protecting global financial platforms, rather than compliance activity, will significantly enhance security efforts. For an industry already burdened by a shortage of adequately skilled individuals, reducing this percentage by streamlining compliance activity is an immediate gain in efficiency and managed risk.

For the regulatory community, Profile use would enhance transparency and improve visibility across institutions, subsectors, third-parties, and across sectors, enabling better analysis and mitigation of systemic and concentration risks.

[2] This predated the Financial Stability Board's announcement in 2017 that 72% of its 25 member jurisdictions were self-reporting that each had plans to issue further cybersecurity regulatory frameworks.

4. Was there broad financial services sector representation in the Profile's development?

Yes, there was broad representation by subsectors (e.g., banking, insurance, asset management, market utilities, broker-dealers) as well as functional roles (e.g., Board Directors, CEOs, CISOs, Chief Information Risk Officers, cyber and privacy attorneys) in the Profile's development.

Starting in Q3 2016, a coalition of trade associations gathered under the Financial Services Sector Coordinating Council (FSSCC)[3] and began working on what would become the Profile, Version 1.0. The 40-50 working sessions over two years included the participation of over 300 individual experts, representing over 150 financial institutions, ranging from community banks and credit unions to large multi-national banks, investment firms, and insurance institutions. These sessions were largely co-led by Josh Magri of BITS (josh.magri@bpi.com), Denyette DePierro of the American Bankers Association (ABA) (ddepierr@aba.com), and the team of framework and standards experts at BCG Platinion, a division of The Boston Consulting Group, led by Nadya Bartol (Bartol.nadya@bcgplatinion.com).

Further input was solicited, received, and integrated from a myriad of U.S. and international financial services regulatory bodies. In April 2018, NIST hosted an open workshop to further develop a scaling methodology for the Profile. Over 100 individuals attended the workshop, with representation from financial services institutions and the state and national supervisory community.

From these sessions, the inputs, feedback, and recommendations provided were reviewed, discussed, and incorporated based on the working group's consensus. The result is the Profile, Version 1.0.

5. What were the objectives and principles used in developing the Profile?

The Profile had to benefit customers, financial institutions, and supervisory agencies worldwide. The working group consensus was that the Profile would have to be –

- Generally applicable and usable by all types of financial institutions, and adaptable based on inherent risk and institutional circumstances;

[3] FSSCC's mission is to strengthen the resiliency of the financial services sector and critical infrastructure against cyber and physical incidents by proactively identifying risks and promoting protection and mitigation, driving preparedness, and coordinating response for the benefit of its consumers, the sector, and the world. Established in 2002, FSSCC is now composed of over 70 member financial institutions, financial utilities, and financial services related trade associations (which, in turn, consist of 1000s of other member institutions). To achieve its mission, FSSCC and its member entities collaborate with appropriate government agencies and governmental bodies to develop and implement a variety of risk management and operational resilience strategies and initiatives. A list of FSSCC member entities can be found on its website: www.fsscc.org.

- Comprehensive in terms of the scope of assessment questions asked and adequately efficient to optimize cybersecurity staff time at the keyboard and supervisors' time conducting higher-value analysis;
- Usable and beneficial for those that are supervised by numerous agencies, in possibly multiple international jurisdictions, and by those that may have fewer supervisors, but want a credible, standardized self-assessment framework; and
- Usable and beneficial for the most interconnected, systemically important institutions, and also among the smaller and least interconnected institutions.

To achieve these objectives, the working group decided to organize the Profile based on widely used frameworks and standards, as well as supervisory guidance and assessment tools, such as the NIST Cybersecurity Framework, the ISO/IEC 27001/2 controls, CPMI-IOSCO, and the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT), among others. This principle of leveraging what existed – and not "starting from scratch" – extended into the creation of the Impact Tiering scaling methodology, with the use of existing criteria for financial sector criticality. It also extended to the formulation of the diagnostic statements, which reference current supervisory expectations. If assessment language existed that did not overlap or have redundant phrasing, that language was used. However, where supervisory agencies used similar, overlapping, or duplicative language or phrasing, the simplest or most ubiquitous language was selected for the Profile.

6. What are the differences between the Profile and the NIST Cybersecurity Framework?

The Profile is a financial services sector-specific extension of the NIST Cybersecurity Framework (NIST CSF)—and other key guidance documents such as ISO and CPMI-IOSCO—to better address the sector's regulatory environment. Like the NIST CSF, the Profile articulates desired security outcomes based on cyber risk management best practices and credible approaches. However, unlike the NIST CSF, the Profile extends the mapping of those risk management activities to sector-specific regulations, guidance, and supervisory materials and includes Diagnostic Statements to aid in assessing a risk management program. It also adds two new functions to NIST's five function design. These two new functions are "Governance" and "Dependency Management," which were added due to their prioritization by the financial services regulators.

In sum, the Profile effectively extends the NIST CSF *vertically*, by adding two additional Functions, and *horizontally*, by adding diagnostic statements that elaborate desired Subcategory outcomes. These expansions align the Profile with the financial services sector's cybersecurity environment, protection needs, and regulatory requirements.

7. Is NIST supportive of this Framework customization?

Yes. With the publication of Profile, Version 1.0, NIST released this a written statement of support:

> "Congratulations on publication of the Financial Services Sector Cybersecurity Profile Version 1.0. NIST encourages customization of our publications in ways that best meet the needs of each user. The Financial Services Sector Cybersecurity Profile Version 1.0 builds upon the Cybersecurity Framework in ways that support the financial services community.
>
> "NIST has found the Financial Services Sector Cybersecurity Profile Version 1.0 to be 1) correct with regard to Cybersecurity Framework Version 1.1, 2) supportive of a risk-based approach to cybersecurity, and 3) one of the more detailed Cybersecurity Framework-based, sector regulatory harmonization approaches to-date.
>
> "NIST is happy to have supported the Financial Services Sector Coordinating Council in developing your work product. As financial services users implement your guidance, let's continue communicating, as user observations will likely inform future versions of the Financial Services Sector Cybersecurity Profile and the Cybersecurity Framework itself."

In addition to the statement, NIST has been an active facilitator and partner in the Profile's development. In May 2017, NIST invited the Profile working group to present an early draft Profile at the annual CSF stakeholders meeting at NIST's Gaithersburg, MD location and posted a summary of the Profile on the NIST CSF webpage. On April 26, 2018, NIST hosted a full-day, open and public workshop, in concert with the Financial Services Sector Coordinating Council, at the U.S. Department of Commerce building in Washington, DC. This workshop considerably advanced the development of the Profile's scaling methodology (what would later become the Profile's Impact Tiering). For a link describing the event, please click here: https://www.nist.gov/news-events/events/2018/04/financial-services-sector-cybersecurity-workshop. Furthermore, NIST invited the working group to present the Profile, Version 1.0 at the NIST risk management conference in Baltimore, MD in November 2018. For a link describing the event, please click here: https://www.nist.gov/news-events/events/2018/11/nist-cybersecurity-risk-management-conference.

8. Which types of institutions can use the Profile?

The Profile is designed for 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 the Profile 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.

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 impacted by a cybersecurity event. These "Impact Tiers" are as follows:

> ***Tier 1: National/Super-National Impact*** – These institutions 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 North American economy, and potentially, the global market.
>
> ***Tier 2: Subnational Impact*** – These institutions provide mission critical services with 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*** – These institutions 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*** – These institutions 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.

Upon determining an institution's impact category, 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.

9. Is the Profile Voluntary? If so, what are some of the benefits of using the Profile?

Usage of the Profile is entirely voluntary. There is no mandate to use the Profile; but there are many benefits to using the Profile.

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;
- 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 the 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 diagnostic assessment questions, 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 would answer a total of 145 questions (9 tiering questions + 136 Diagnostic Statement questions). As compared to another widely-used assessment tool's 533 questions, this represents ***a 73% reduction.***
- **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 would answer 279 questions (2 tiering questions + 277 Diagnostic Statement questions) as compared to the other widely-used assessment's 533, ***a 49% reduction***.

Additional Benefits: While increased time and focus on cybersecurity projects and activities is a substantial benefit, continued use of the Profile would bring additional benefits. Immediate benefits for financial institutions include:

- Enhanced internal and external oversight, due diligence and risk identification using consistent terms and concepts;
- More efficient third-party vendor management review and oversight;
- Greater intra-sector, cross-sector and international cybersecurity collaboration due to the common use of ISO standards, CPMI-IOSCO and the NIST Cybersecurity Framework; and
- Encouraging innovation and adoption of emerging technology, as FinTech firms and startups can more readily demonstrate adherence to financial services sector cybersecurity requirements and supervisory expectations.

Benefits to Regulatory Community

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

- 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 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.

10. What are some of the benefits to Community Banks (or less inherently risky institutions) in using the Profile?

Mergers and Acquisition/Institutional Safety and Soundness. A common approach to cybersecurity is important for M&A purposes. When evaluating acquisition targets — even those located within a 1-state footprint—cyber readiness and compliance gaps are a primary concern. Cyber alignment and maturity would be easier to evaluate and compare across institutions with a common approach, such as the Profile.

Multibank or Financial Services Holding Company. A small community bank may be part of a multibank holding company, with sister banks holding differing charters and/or financial services affiliates subject to SEC, or other non-bank oversight. A common approach to cyber

within the financial services family of companies is a better use of resources and would make all affiliated entities safer.

Bank Growth and Evolution/Safety and Soundness. A bank's ability to evolve and grow would be aided by a common cyber approach. If a single-state bank wants to expand operations to a second state, change charters, acquire another institution—bank or nonbank financial company—a common cyber approach facilitates a bank's ability to be responsive to market conditions and strategic planning.

Interconnectedness/Safety and Soundness. As the supervisory environment becomes more focused on third-party risk and vulnerability by interconnectedness, banks of all sizes could be asked to demonstrate a robust approach to cybersecurity before participating in certain payment activities, high-risk banking transactions, or lower premium cybersecurity insurance policies. A common approach to cybersecurity, based on the Profile, Version 1.0, will allow banks of all sizes and business models to evaluate their cyber program—and the cyber program of other institutions— for threats, vulnerabilities, and defenses, in order to make an informed business decision about how, and with whom, to partner.

11. <u>What are the use cases for the Profile?</u>

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.

> ***Profile as Third-Party Risk Management Tool:*** Similar to 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, internally and externally.

12. Is the Profile widely supported by the financial services sector?

Yes, the Profile has wide financial services sector support. It has the support of the Financial Services Sector Coordinating Council (FSSCC), financial institutions, and financial services trade associations representing financial institutions from each subsector.

Developed and released by the FSSCC, the Profile is also supported by a coalition of trade associations. In alphabetical order, this coalition is composed of the following trade associations (and growing):

- The American Bankers Association (ABA);
- The Bank Policy Institute (BPI), and its technology policy subdivision –
  - BITS – Business, Innovation, Technology, Security;
- The Futures Industry Association (FIA);
- The Global Financial Markets Association (GFMA), and its member associations of –
  - The Association for Financial Markets in Europe (AFME),
  - The Asia Securities Industry & Financial Markets Association (ASIFMA), and
  - The Securities Industry and Financial Markets Association (SIFMA);
- The Institute of International Bankers (IIB); and
- The Institute of International Finance (IIF).

Adding Your Trade Association's Support: We are collecting logos of trades that are supportive of the Profile. By allowing usage of the logo on the Profile and Profile related documents, it means that the trade association and its member institutions recognize:

> *The Financial Services Sector Cybersecurity Profile represents a comprehensive compilation of cybersecurity risk management best practices that could represent a basis for regulatory/supervisory harmonization for the financial services sector.*

For more information or to lend your support, please contact Profile leads: Josh Magri of Bank Policy Institute (BPI) - BITS and Denyette DePierro of the American Bankers Association.

Josh Magri
Senior Vice President, Counsel for Regulation & Developing Technology
Josh.Magri@BPI.com
Bank Policy Institute (BPI) – BITS

Denyette DePierro
Vice President & Senior Counsel
Center for Payments and Cybersecurity
ddepierr@aba.com
American Bankers Association

13. What do supervisory and other agencies think of the Profile?

Numerous U.S. federal regulators and agencies have encouraged its development and announced their public support for the Profile and its use at its release event on October 25, 2018.

Additional statements of support will be posted in the coming days.

14. Are financial institutions using the Profile already?

Yes, financial institutions are already using the Profile. A number of those institutions described their usage at the Profile's release event on October 25th. Others volunteered to use earlier drafts alongside other frameworks and regulatory tools to compare and generate feedback. The feedback provided proved invaluable and led to the incorporation of enhancements into the Profile, Version 1.0.

15. Is the Profile mapped to all existing global cybersecurity regulations, guidance, etc.? Are additional supervisory mappings being considered?

The Profile's mappings are comprehensive, but they are not exhaustive. The Profile has mapped to and integrated numerous global standards and supervisory expectations, including the ISO/IEC 27001/2 controls, CPMI-IOSCO's "Guidance on cyber resilience for financial market structures," among others. More such mappings, however, have been requested. To satisfy these requests, the coalition has committed to map regulations, frameworks, guidance, etc., from leading jurisdictions on a rolling basis in the months that immediately follow Profile, Version 1.0's release.

To the extent that you believe that a Supervisory issuance should be included in a future version, please submit suggestions to ProfileComments@bpi.com. Such suggestions will be considered using a multi-stakeholder process similar to the one used in developing Version 1.0 of the Profile.

16. What is the governance structure and the process for Profile maintenance and updates going forward? Is there a Roadmap for future Profile considerations and updates?

Future Profile Governance and Profile Maintenance: The Financial Sector Coordinating Council (FSSCC), the trade associations, financial institutions, and other Profile development stakeholders recognize that future maintenance of the Profile is essential for its ultimate success. Numerous trade associations and financial institutions involved in the Profile's development are forming a sustained coalition to manage Profile update activities and to educate and engage jurisdictions around the world on its benefits and usage. Interested parties

will continue committing resources, such as their own subject matter experts and expertise, full time personnel, and funds for external experts and advisors.

This coalition has also committed to a 2-3 year update cycle to iterate a new, full version similar to the cycles used by other standards bodies, such as the National Institute of Standards and Technology (NIST) and International Standards Organization (ISO) for a full version. The coalition has also committed to more flexible update timeframes to include additional global supervisory expectations as well as any newly issued supervisory expectations.

The coalition recognizes that users may suggest potential enhancements and new cyber risk management concepts between Profile versions. As these recommendations surface, the coalition 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 will include a review by a coalition executive committee and other stakeholders, as appropriate, as was done to develop the Profile from concept to a Version 1.0.

The Roadmap: In addition to the release of the Profile, FSSCC has also generated "A Roadmap Forward" (Roadmap). The Roadmap is a companion document articulating topics to be addressed and planned activities occurring between successive versions. These topics and activities are listed in priority order and may change as circumstances change. Accordingly, please continue to check the Roadmap regularly. It can be found on the same webpage as the Profile.

17. Can I add our support to the Profile efforts?

Yes, we are continuing to build our coalition of trade associations and financial institutions. For more information or to lend your support, please contact Profile leads: Josh Magri of Bank Policy Institute (BPI) - BITS and Denyette DePierro of the American Bankers Association.

Josh Magri
Senior Vice President, Counsel for Regulation & Developing Technology
Josh.Magri@BPI.com
Bank Policy Institute (BPI) – BITS

Denyette DePierro
Vice President & Senior Counsel
Center for Payments and Cybersecurity
ddepierr@aba.com
American Bankers Association

18. <u>Finally, are there Terms of Use Applicable to Profile usage?</u>

Yes, this work is licensed under the Creative Commons Attribution-NonCommercial-NoDerivatives 4.0 International License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc-nd/4.0/ or send a letter to Creative Commons, PO Box 1866, Mountain View, CA 94042, USA.