CYBER RISK
INSTITUTE

It is an exciting time for CRI as we enter 2022. We will be emerging as a stand-alone entity, building a digital platform to benefit our members, and continuing to grow and maintain the Profile to fit the needs of all stakeholders in the financial services sector around the world. As we release version 1.2 of the Profile, we wanted to remind our members of what we have done with their support and assistance and what we have planned for future versions of the Profile.

Version 1.2

The latest version of the Profile includes several mappings of regulatory issuances impacting our members around the globe, as well as a substantial "quality-of-life" improvement with the release of the Profile Workbook. The Profile Workbook contains response guidance and suggestions for effective evidence to support an organization's response to the Diagnostic Statements. The regulatory issuances that have been mapped to the Profile and included in the Financial Sector References Column of the Profile Spreadsheet include:

- European Central Bank's "*Cyber resilience oversight expectations for financial market infrastructures"* (published December 2018);
- European Banking Authority's (EBA) "*EBA Guidelines on ICT and security risk management"* (published November 2019);
- A more granular mapping to the New York State Department of Financial Services' (NYDFS) 23 NYCRR Part 500, entitled "*Cybersecurity Requirements for Financial Services Companies"* (published March 2017);
- A more granular, bidirectional mapping to the U.S. Federal Financial Institutions Examination Council's (FFIEC) *"Cyber Assessment Tool;"* and
- The FFIEC's updated *"Business Continuity Management"* booklet to its IT Examination Handbook (update published November 2019).

With the release of the Profile version 1.2, CRI is fulfilling its promise to keep the Profile evergreen and in sync with regulatory bodies around the globe.

Version 2.0

When CRI was launched in 2019, we recognized the need for keeping the Profile relevant and responsive to the current regulatory environment without disrupting organizations use of the Profile. Thus far, we have not edited the Diagnostic Statements so that organizations could become comfortable with the statements and integrate them into their compliance and operational frameworks. With version 2.0, we will be addressing Diagnostic Statements to ensure clarity and coverage. Our approach is to ensure that the Profile is covering those areas of cybersecurity and technology control programs that our members want and need.

By design, the Profile is not intended to be exhaustive of all cybersecurity and technology control aspects that could be included in a framework. The goal is to cover approximately 85% of the issues with which 85% of the regulators around the world were concerned. This creates a solid baseline for our

members to create effective security and control programs while providing flexibility to build according to their business needs and the specific regulatory concerns of their supervisors.

However, through our mapping efforts, we have identified areas of importance to multiple supervisors that, if incorporated, would extend the Profile's utility to beyond purely cyber risk management. CRI will consider the areas that may be most useful to the financial sector by reflecting regulatory priorities while not overburdening the Profile.

Additional changes to the Profile in Version 2.0 will likely include:

- Clarifying and enhancing Diagnostic Statements, particularly in the Supply Chain/Dependency Management function, to ensure that each Diagnostic Statement adds value to a risk management program.
- Structural additions to include Categories, Subcategories, and Diagnostic Statements related to technology controls, project management, and third-party risk management.
- Ensuring the initial impact tiering questionnaire reflects appropriate international concerns when determining the impact of organizations to the financial sector.
- Additional mappings:
    - Hong Kong Monetary Authority's (HKMA) Cybersecurity Fortification Initiative (CFI) 2.0 and the associated "*Cyber Resilience Assessment Framework"* (C-RAF) (CFI 2.0 published November 2020, effective January 2021);
    - Monetary Authority of Singapore's (MAS) "*Technology Risk Management Guidelines*" (published January 2021) and its "*Notice 655 Cyber Hygiene*" (published in August 2019);
    - People's Bank of China's Multi-Level Protection Scheme (MLPS) 2.0 at Level 3, which includes the *"Baseline for Classified Protection of Cybersecurity," "Technical Requirements of Security Design for Classified Protection of Cybersecurity," and "Information Security Technology-Evaluation Requirements for Classified Protection of Cybersecurity";*
    - Reserve Bank of India's (RBI) June 2016 Circular, entitled "*Cyber Security Frameworks in Banks";*
    - Securities and Exchange Bank of India's (SEBI) December 2018 Circular, entitled "*Cyber Security & Cyber Resilience framework for Stock Brokers / Depository Participants";*
    - U.S. Securities and Exchange Commission (SEC) Division of Examinations' (formerly the Office of Compliance Inspections and Examinations) 2020 Examination Observations, entitled "*Cybersecurity and Resilience Observations"; and*
    - U.S. Federal Financial Institutions Examination Council's (FFIEC) Information Technology Examination June 2021 Handbook, entitled "*Architecture, Infrastructure and Operations."*

<u>Future Developments (2022 and beyond)</u>

One of the most exciting developments that we are looking forward to in 2022 is the creation of our digital platform that should greatly improve the way our members interact with the Profile. The platform will enable automation and represents a migration away from spreadsheets (that will remain

available to the public on our website). The platform will enable our members to integrate their Profile work into their GRC tool of choice and make updating and maintaining their Profile dataset much more intuitive and efficient. The platform's availability is expected mid-2022.

We continue to develop a maturity methodology to enable how an organization can demonstrate how much of the Profile they have integrated into their own security program, as well as the ability for our members to benchmark, or measure, themselves against their peers. We expect to release a public version of the maturity methodology and enable benchmarking through the platform by the end of 2022.

In addition to the platform, we have been working on additional extensions of the Profile for cloud environments and for third party risk management. The cloud extension will leverage the Cloud Security Alliance's Cloud Control Matrix (CCM) and provide guidance for how organizations can implement a shared responsibility model in various implementation environments (SaaS, PaaS, and IaaS). The third-party risk management extension will demonstrate the overlap of the Profile with a robust third-party risk management framework developed by one of our key partners, the Securities Industry and Financial Markets Association (SIFMA) and its members. The Cloud extension has planned availability in early 2022, while the third party extension should be available by the end of that year.

Finally, CRI members have asked us to engage with a number of other standards development organizations to discuss possible integrations of their works. CRI will make more specific announcements in the months to come.