The Financial Services Sector Cybersecurity Profile (Profile)
- The Roadmap Forward -

The release of the Profile, Version 1.0, is just the beginning of this initiative. To ensure that the Profile is properly maintained and updated to meet user needs and the evolving supervisory landscape, this companion Roadmap will articulate 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.

(1) **Profile Governance and Maintenance 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.

(2) **Mapping of Additional Global Supervisory Regimes:** The Profile has already mapped to and integrated numerous global standards and supervisory expectations, including the

ISO 27000 series of 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.

(3) **Examination and Possible Inclusion of Further Elements of Operational Resiliency:** The field of cyber risk management is maturing, and with maturation, there has been an increased focus on the intersection of cybersecurity with overall operational resilience. Supervisory agencies are increasingly focusing on resilience (e.g., G-7 Finance Ministers and Central Bank Governors "Next Steps for Strengthening International Financial Sector Cyber Resilience" and companion documents and the European Central Bank's public consultation on "Cyber Resilience Oversight Expectations"), as are standards bodies, such as NIST (e.g., Draft NIST Special Publication 800-160, vol. 2, "Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems).

Because these consultations are in their infancy and because operational resiliency includes concepts beyond cybersecurity, the coalition recognizes that an intensive review of Subcategories and Diagnostic Statements will be required before those concepts might be appropriately incorporated. As such, all efforts will be made to ensure operational resiliency – particularly systemic resiliency – is examined and addressed for future Profile updates without diverging inappropriately from existing supervisory requirements and the underlying CPMI-IOSCO/NIST Cybersecurity Framework architecture and taxonomy.

(4) **Enhanced Mapping Features and Automation:** The coalition recognizes that usage of the Profile would be enhanced with automated functions and features. With the release of Profile, Version 1.0, FSSCC is providing the Profile in PDF and a more automated Excel Spreadsheet version that could be used for self-assessment purposes. At the request of those that have helped develop a Version 1.0, the coalition envisages enhancements in automation, which might include an enhanced user interface, hyperlinks to specific supervisory references, and other informative references.

If you have recommendations to enhance the Profile and/or supplement the Roadmap, please feel free to email ProfileComments@BPI.com or 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

Because this Roadmap is subject to amendment, please check back regularly.