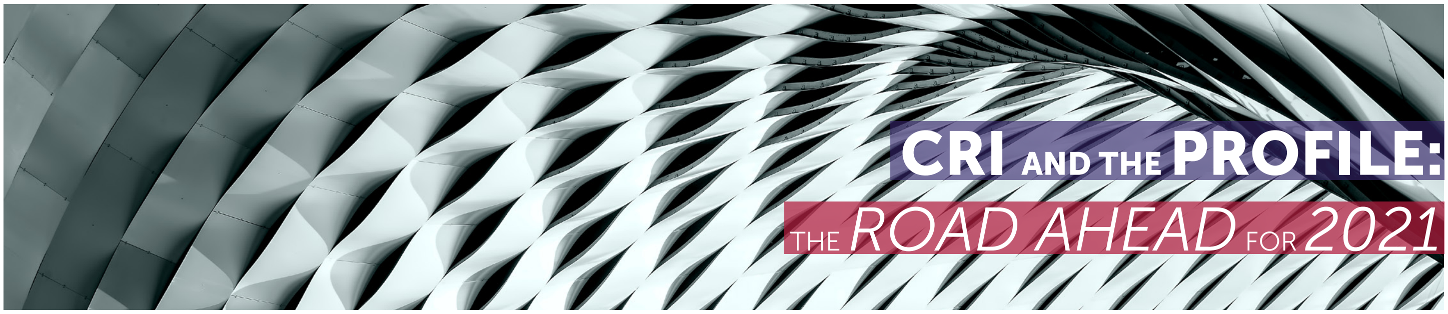
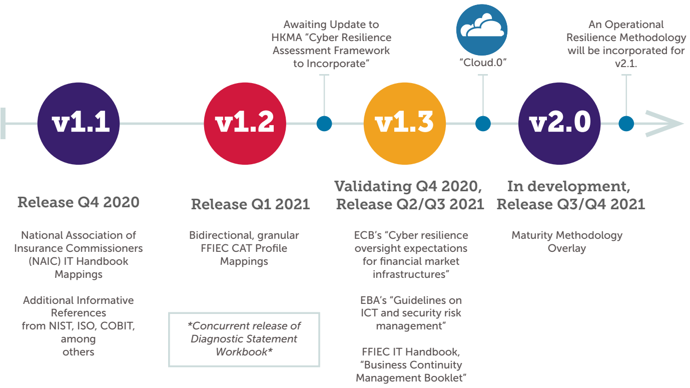


CRI AND THE PROFILE: THE ROAD AHEAD FOR 2021

As the Cyber Risk Institute (CRI) enters its second year, our CRI Cybersecurity Profile ("Profile") Version 1.1 released in November 2020 will continue to evolve. As announced last year, CRI is on track to release a Version 1.2 in early 2021, followed shortly by a Version 1.3, and a further, more robust update in Version 2.0 by the end of the year. During this period, CRI expects to further develop and publish a Cloud Controls version of its Profile. This reflects our commitment to maintain and update the Profile to meet user needs and the evolving supervisory landscape. We have worked closely with industry leaders and regulators to identify possible integrations for the Profile. Under the leadership of our member organizations, we have prioritized them and already initiated integration efforts.


Awaiting Update to HKMA "Cyber Resilience Assessment Framework to Incorporate"
"Cloud.0"
An Operational Resilience Methodology will be incorporated for v2.1.
v1.1
v1.2
v1.3
v2.0
Release Q4 2020
Release Q1 2021
Validating Q4 2020, Release Q2/Q3 2021
In development, Release Q3/Q4 2021
National Association of Insurance Commissioners (NAIC) IT Handbook Mappings
Additional Informative References from NIST, ISO, COBIT, among others
Bidirectional, granular FFIEC CAT Profile Mappings
Concurrent release of Diagnostic Statement Workbook
ECB's "Cyber resilience oversight expectations for financial market infrastructures"
EBA's "Guidelines on ICT and security risk management"
FFIEC IT Handbook, "Business Continuity Management Booklet"
Maturity Methodology Overlay

This update provides an understanding of what the future of the Profile holds and insight into CRI activities in the months ahead.

Profile Governance and Maintenance

Ongoing maintenance of the Profile is core to our efforts and is led by our members. The coalition of organizations which came together to create the Profile forms the original core of this membership, as it has continued to grow throughout this first year. These industry leaders have devoted time and resources molding the future course of the Profile. This includes prioritizing standards and regulatory regime integrations through participation in our Standards Committee, leading the development of an online Profile platform through our Finance and Operations Committee, validating Profile mappings as part of our open working groups, or serving as an industry representative during our engagements with senior regulatory officials.

CRI's membership is representative of the full range of firms across the financial services industry. Members include community institutions to non-US based, global institutions. Such representation assures that the Profile continues to provide value to each segment of the sector.

As our members and the wider Profile user-base offer recommendations on how to grow the Profile, CRI evaluates their applicability within the regulatory landscape, their utility to a cyber risk management program, and the feasibility of incorporation into the Profile's next version. This process will continue as we move toward Version 1.2 and beyond.

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. For Version 1.1, CRI added the National Association of Insurance Commissioners' own mapping of its Financial Condition Examiners Handbook/Exhibit C: Evaluation of Controls In Information Technology to the Profile; as well as additional "Informative

References" for the Functions "Governance" and "Supply Chain/Dependency Management," better connecting those functions and related diagnostics to widely used industry standards such as ISO, COBIT, and NIST 800-53. To continue to meet industry's needs, CRI is mapping additional regulations, frameworks, guidance, etc., from leading jurisdictions on a rolling basis, incorporating these in future versions of the Profile.

Version 1.2 will include a more granular, bidirectional mapping of the FFIEC Cybersecurity Assessment Tool (CAT) to the Profile and the Profile to the CAT. this will provide a smoother exam experience for those insitutions that face regulatory exam teams with a history of using the CAT. These mappings will be released alongside a diagnositc statement workbook. This workbook provides robust interpretative guidance for each diagnostic statement and also gives examples of effective documentation and evidence that firms can include to support their responses to particular diagnostics.

In preparation for Version 1.3, CRI has mapped, and is currently validating mappings for, the European Central Bank's "cyber resilience expectations for financial market infrastructures"; the European Banking Authority's "Guidelines on ICT and security risk management"; and the FFIEC's IT Handbook on "Business Continuity Management." These are scheduled to be finalized in Q4 of 2020 and released in Q2/Q3 of 2021. We are also working on a maturity methodology, which has been circulated for stakeholder comment and will be incorporated into an expected Version 2.0 release in Q3/Q4 of 2021.

In addition to the above, the CRI Management Board has also approved mapping and incorporation of the following Standards Committee prioritizations:

United States-based Priorities:

- Cloud controls to further develop a Cloud Control version of the Profile
- Any U.S. financial services regulatory agency rulemakings pertaining to incident response and recovery
- U.S. regulatory frameworks on Operational Resilience.

Global Regulatory Priorities:

- People's Republic of China "Multi-level Protection for Cybersecurity" (MLPS 2.0 series of national standards), 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 June 2016 Circular, "Cyber Security Frameworks in Banks"
- Securities and Exchange Bank of India December 2018 Circular, "Cyber Security and Cyber Resilience Framework for Stock Brokers/Depository Participants"
- SWIFT Customer Security Programme

Operational Resilience

On October 30, 2020, three leading U.S. financial services regulatory agencies – the Federal Reserve, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency - jointly issued a report entitled "Sound Practices to Strengthen Operational Resilience." This document details "practices to increase operational resilience that are drawn from existing regulations, guidance, statements, and common industry standards" to help large banks increase operational resilience in the face of risks such as cyberattacks, natural disasters, and pandemics. Though it does not include any new regulations, it is nonetheless a clear indication of the future of efforts to address operational resilience in the financial services industry. Importantly, this document mirrors the IOSCO/NIST-based structure of the CRI Profile – providing further evidence of the effectiveness of an approach which combines industry-best practices with regulatory requirements.

CRI will continue to watch discussions around operational resilience closely. Because these consultations are in their infancy and because operational resilience includes concepts beyond cybersecurity, CRI 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 resilience is examined and addressed for future Profile updates (potentially a Version 3.0) without diverging inappropriately from existing supervisory requirements and the underlying CPMI-IOSCO/NIST Cybersecurity Framework architecture and taxonomy. All of this will be significantly impacted by responses to and lessons learned from the COVID-19 pandemic.

Enhanced Mapping Features and Automation

CRI is working to enhance the Profile with automated functions and features, to create a cloud-based platform with a simple user interface. Currently, CRI provides the Profile only as a free macro-enabled Microsoft Excel Spreadsheet, which can be used for self-assessment purposes. However, our Finance and Operations Committee has been conducting an analysis of potential vendors to develop an online Profile platform. This effort has helped to crystalize the requirements needed for a formal Request for Proposal (RFP) to be issued in the coming year.