CYBER RISK INSTITUTE

The CRI Profile User Guide

Guidance for Using the CRI Profile v2.0 Workbook

Last updated: February 2024

Cyber Risk Institute
Washington, D.C.

CyberRiskInstitute.org

CYBER RISK INSTITUTE

THE CRI PROFILE VERSION 2.0

An Overview and User Guide

INFORMATIONAL PURPOSES ONLY: The information contained within this spreadsheet document and in related Profile documents are intended for informational purposes only. The information contained herein is provided on an "as is" basis without warranty of any kind, either express or implied. CRI assumes no liability or responsibility for any errors or omissions in the content of this document. Please be sure to check for the most recent versions at https://cyberriskinstitute.org.

Talk with your regulator: by including mappings and references to various regulatory agencies' publications, that does not mean, nor should it be construed, that the referenced agency necessarily supports, or endorses, the mappings or the Profile's use for regulatory purposes. Additionally, use of the Profile does not limit what a supervisor can review or requires. Rather, the Profile enables financial institutions to confidently produce baseline evidence for review and more quickly respond to iterative and follow-up questions from examiners.

1 Introduction

Cyber Risk Institute (CRI) has developed CRI's Profile v2.0 framework to create an efficient approach to technology and cybersecurity risk management that effectively counters dynamic and evolving threats and provides adequate assurance to government supervisors. This is an updated version of the CRI Profile ver. 1.2.1 that serves to provide additional guidance for organizations to align with technology and cybersecurity regulatory expectations and authorities. The Profile also provides a flexible structure to inform the development of a cybersecurity program according to business needs and specific regulatory expectations within an individual organization, vocabulary, and taxonomy.

Through collaboration and consensus between financial institutions, this document seeks to develop both a self-assessment and tool for institutions to create a common baseline security threshold, and provide a common supervisory engagement approach among state, federal, and international regulatory bodies. This is possible because the Profile has been mapped to and integrated numerous global standards and supervisory expectations, including those from Japan, the European Union, Australia, Singapore, and the United States, among others.

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. Upon determining an institution's Impact Tier, the Profile is customized to meet the institution's likely technology and cybersecurity risk, and applicability of the CRI Profile v2.0 diagnostic statements. CRI Profile v2.0 provides guidance for benchmarking an individual institution's program with the Profile's recommended practices, to

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.

2 Acknowledgements

The CRI Profile is the result of tremendous effort from many organizations of varying sizes and complexities. We want to extend our gratitude to the financial institutions, regulatory groups, and other organizations who contributed to this initiative. We want to particularly thank BCG Platinion, which provided initial support to the Profile's development, and EY, which provided expertise and manpower to this important sector initiative. We also want to thank our 50+ member organizations, our CRI Board of Directors, which provided the strategic guidance, and the CRI Profile Architecture Working Group, which reviewed and validated all of the Profile's content and mappings. Finally, we want to acknowledge CRI's John Goodman and Emily Beam for their tireless thought leadership, contracting oversight, and member engagement on the largest Profile update to date.

3 Document Structure

The CRI Profile v2.0 consists of multiple worksheet tabs to identify regulatory expectations within various frameworks and align them to the CRI Profile v2.0.

Worksheet	Worksheet Description	Purpose
User Guide	Introduces the CRI Profile v2.0, its structure, and provides guidance on how to use the document.	Provides guidance on how to use the CRI Profile.
Impact Tiering Questionnaire	This worksheet contains the CRI Impact Tiering Questionnaire, which will prompt a user to answer a set of self-assessment questions to customize the Profile assessment based on an individual institution's risk and activities. When the organization's Tier level has been determined using the questionnaire, the value should be entered into cell I2 in the Profile Assessment worksheet.	Provides an institution the ability to adjust the number of diagnostic statements applicable to identify gaps and implement a plan to remediate depending on its risk posture in recognition that each organization has a different risk environment and tolerance.
CRI Profile v2.0 Structure	This worksheet contains the CRI Profile v2.0 diagnostic statements grouped by Function, Category, and Subcategory. It indicates the applicability of each diagnostic statement to each Tier level and tag. Tags provide an overview of key words that are applicable to each diagnostic statement so	Provides a connection between seven functions of (1) Govern, (2) Identify, (3) Protect, (4) Detect, (5) Respond, (6) Recover, and (7) Extend to Diagnostic Statements and existing financial sector compliance requirements and sector-agnostic informative references. It also provides a view for an individual institution to filter by Tier level and tag to view the applicable CRI Profile v2.0 diagnostic statements. Its flexible structure

Worksheet	Worksheet Description	Purpose
	organizations can easily filter and categorize diagnostic statements.	makes the Profile possible to address the needs of industries beyond financial services.
CRI Profile v2.0 Assessment	This worksheet contains the CRI Profile v2.0 diagnostic statements grouped by Function, Category, and Subcategory. It indicates the applicability of each diagnostic statement to each Tier level. Each statement is given an assessment rating with a supporting rationale and evidence provided to justify the rating given.	Provides a connection between seven functions of (1) Govern, (2) Identify, (3) Protect, (4) Detect, (5) Respond, (6) Recover, and (7) Extend into Diagnostic Statements with existing compliance requirements and informative references which makes it flexible to address the needs of industries beyond the financial services. It also provides a view for an individual institution to filter by Tier level and tag to view the applicable CRI Profile v2.0 diagnostic statements. In addition, it gives the financial institutions the ability to view their posture against the CRI Profile to be utilized in their decision-making process.
Assessment Response Summary	Provides a summary of the financial institution's responses to the assessment scores for each function, category and subcategory of the CRI Profile by completing the assessment ratings in the "CRI Profile v2.0" tab.	Provides a mechanism for financial institutions to understand their posture against the CRI Profile to enable for informed decision-making and targeted improvements.
Diagnostic Statements by Tag	This worksheet contains the CRI Profile v2.0 diagnostic statements grouped into subject tags.	Provides a different connection between the diagnostic statements separated by their aligning topic so organizations have the ability to list, sort and filter diagnostic statements by these subject tags.
Subject Tag List	This worksheet contains the number of diagnostic statements within each of the subject tags.	Provides an overview of the amount of diagnostic statements each subject tags covers.
Profile v.1.2.1 Mapping	This worksheet provides a mapping of the change status between CRI Profile v1.2 and CRI Profile v2.0.	Provides a full picture of all the changes made to the diagnostic statements from v1.2 to v2.0 to allow for a clear understanding of each change.
Catalog of Mapped Regs	This worksheet contains a catalog of frameworks mapped to the CRI Profile v2.0, including issued by, name of issuance, region, issue date, and description.	Provides an overview of all supervisory expectations and other industry standards that have been mapped to the CRI Profile v2.0 diagnostic statements.

Worksheet	Worksheet Description	Purpose
FFIEC CAT to Profile Mapping	Provides a detailed mapping of the FFIEC CAT to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
Profile to FFIEC CAT Mapping	Provides a detailed mapping of the FFIEC CAT to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
FFIEC AIO Mapping	Provides a detailed mapping of the FFIEC AIO Handbook to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
FFIEC BCM Mapping	Provides a detailed mapping of the FFIEC BCM Handbook to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
OCC CSWP - CRI Profile v2	Provides a detailed mapping of the OCC CSWP to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
SEC Aug 2023 Mapping	Provides a detailed mapping of the SEC August 2023 Disclosure, etc. Rule to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
NYDFS Mapping	Provides a detailed mapping of NYDFS Part 500 to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
EBA Mapping	Provides a detailed mapping of the EBA's guidelines to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
ECB CROE Mapping	Provides a detailed mapping of the ECB's CROE guidelines to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
MAS TRMG and CHN to CRI Profile	Provides a detailed mapping of the MAS TRMG and CHN to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
JFSA Mapping	Provides a detailed mapping of JFSA's guidelines to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
CISA CPG 1.0.1 Mapping	Provides a detailed mapping of the CISA CPG 1.0.1 to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.
NIST Ransomware Profile	Provides a detailed mapping of the NIST Ransomware Profile to the CRI Profile v2.0.	See worksheet Catalog of Mapped Regs for document details.

4 How to Use the Document

4.1 Impact Tiering Questionnaire

The Impact Tiering Questionnaire is the first worksheet that will be accessed by the financial institution to self-assess and customize the Profile based on an individual institution's risk and activities. The Profile may assist

institutions in assessing their technology and 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.

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** – These institutions are designated *most critical* by one or more global regulatory agencies and/or bodies (e.g., the Basel Committee's Global Systemically Important Bank (GSIB) designation or Executive Order 13636's 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 a national 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.

Once an institution determines its Impact Tier by completing the Impact Tiering Questionnaire, the institution should assess itself against the corresponding Diagnostic Statements, found within the CRI Profile v2.0. This is done by entering the organization's Tier level, as determined by using the questionnaire, into cell I2 of the CRI Profile v2.0 Assessment worksheet. Doing this will set the indicators of which Diagnostic Statements need to be assessed, and which are Not Applicable, in column I.

Based on self-assessment of the diagnostic statements, the institution should be able to identify shortcomings and gaps within its technology and cybersecurity risk management governance, processes, capabilities, and regulatory compliance posture. Plans should develop and implement a plan to close these gaps and address shortcomings to satisfy the expectations of its determined Impact Tier.

4.2 CRI Profile v2.0 Assessment Worksheet

Columns A - D:

Hierarchically organized and labeled with the various Functions (F), Categories (C), Subcategories (S), and Diagnostic Statements (DS) to provide the financial institution a way to navigate for the information required.

There are seven overarching functions: (1) Govern, (2) Identify, (3) Detect, (4) Protect, (5) Respond, (6) Recover, and (7) Extend. These are adapted from the NIST Cybersecurity Framework, CPMI-IOSCO, and

financial sector supervisory guidelines 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 technology and cybersecurity risk management program.

Each Subcategory is associated with at least one Diagnostic Statement, which are designed to assess an institution's own technology and cybersecurity risk management programs.

These columns reflect the CRI Profile v2.0 Functions, Categories, Subcategories, and Diagnostic Statements that institutions use to assess their technology and cybersecurity risk management programs."

Columns E - H:

Identifies the in-scope Functions, Categories, Subcategories, and Diagnostic Statements based upon the different Impact Tiers."

Columns I - K (To be completed by the financial institution):

Financial institutions should navigate to Diagnostic Statements indicated with ""To Be Assessed"" to identify the in-scope Diagnostic Statements for their Impact Tier. After assessing the institution's cybersecurity program, use the drop-down selection and respond with the appropriate implementation status:

Yes: All of the control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis, and are demonstrated to be designed and operating reliably in the organizational environment.

Yes-Risk Based: All of the control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis and are demonstrated to have been designed and operating reliably for the highest-risk assets, or highest-risk control functions, in organizational environment.

Yes-Compensating Control: Achievement of the control outcome(s) has/have been met by using compensating controls.

No: The control outcome(s) described in the Profile Diagnostic Statement have not been meaningfully implemented.

Partial: A meaningful subset of the control outcome(s) described in the Profile Diagnostic Statement are assessed and/or tested on a regular basis and are demonstrated to have been designed and operating reliably in the organizational environment.

To Be Determined: The achievement of outcome(s) for the Profile Diagnostic Statement has not yet been assessed or determined.

Not Applicable: The Profile Diagnostic Statement has been determined to be not applicable to the with other relevant stakeholders within the institution to determine the most accurate response."

Columns L - M:

Column L provides explanatory guidance for each diagnostic statement for the financial institution to consider when completing the assessment. Column M provides examples of commonly used artifacts and evidence to support an assessment of each given diagnostic statement."

Column N:

Reflects the CRI Profile v2.0 subject tags that apply to the given Diagnostic Statement based upon the information reflected within the statement.

4.3 Framework Mappings (Green Tabs)

This section of the document offers comprehensive mappings of the CRI Profile to various financial services regulatory documents and industry standards. The worksheet "Catalog of Mapped Regs" contains a listing of the source documents for which Profile mappings are provided. These mappings serve as a valuable resource for organizations aiming to achieve a deeper understanding of the correlation between these frameworks and to simplify their compliance efforts across different regulations and industry standards. Each worksheet supports the mapping of each Profile Diagnostic Statement allowing organizations to efficiently compare and navigate the interrelated controls found within each framework document.

4.4 Summary of Changes from Profile v1.2.1 to Profile v2.0

Listed below will be the summary of changes from Profile v1.2.1 to Profile v2.0:

- The Profile structure view no longer has merged cells so it is more compact, easier to filter and sort through. The Outline ID column has been added to re-sort the Profile structure correctly. The Level field allows you to filter by functions, categories, subcategories, and diagnostic statements.
- There is a direct mapping to the NIST CSF v2, with an added function, called "Extend," for third-party lifecycle management.
- Subject tagging has been introduced with 108 different tags currently existing, providing the ability to list, sort, and filter diagnostic statements by these subject tags.
- Simplified assessment responses now exist with fields for an assessment rationale and supporting evidence, as well as a new response distribution summary sheet to help institutions create a snapshot of their CRI Profile v2.0 alignment.
- The color scheme is compliant with accessibility standards established under the *Americans with Disabilities Act.*
- Subcategory names have been added in both the “Profile Structure” worksheet and “Assessment worksheet” for easier navigation.
- New mapping relationships have been added with a full mapping view of Profile v1.2.1 to v2.0.

5 Re-evaluation

An individual institution should repeat 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;
- Change in Impact Tier; and/or
- A regulatory or supervisory body believes that the institution's self-assessed Impact Tier is inaccurate or has changed.

6 Points of Contact and Further Information

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. Frequently Asked Questions can be found on CRI's website at https://cyberriskinstitute.org/the-profile/profile-faq/

Josh Magri
President
membership-cri@CyberRiskInstitute.org
Cyber Risk Institute (CRI)