CYBER RISK INSTITUTE

The CRI Profile Fact Sheet

Highlights of CRI Profile version 2.0 Changes

Last updated: February 2024

Cyber Risk Institute
Washington, D.C.

CyberRiskInstitute.org

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.*

CYBER RISK INSTITUTE

THE CRI PROFILE VERSION 2.0 FACT SHEET

The Cyber Risk Institute (CRI) is pleased to release version 2.0 of the CRI Profile—the most expansive revision to date with an expanded scope, new features, and double the mappings to regulations and best practices.

1 Tied to NIST CSF

In developing version 2.0, CRI was committed to remain tightly aligned with prevailing cybersecurity standards, including the National Institute of Standards and Technology's (NIST) Cybersecurity Framework (CSF). CRI Profile version 2.0 is fully aligned with the latest CSF version 2.0 released on February 26, 2024.

CRI has been engaged in the CSF update process by submitting responses to requests for information and participating in public workshops when asked. In fact, NIST referenced CRI in its CSF 2.0 Concept Paper and added the new Govern function focused on cybersecurity governance, which the financial sector sees as a critical element of sound cybersecurity.

Additionally, NIST better addressed cybersecurity supply chain issues by creating a subcategory for cybersecurity supply chain risk management within the Govern Function. This is one area of difference between the NIST CSF version 2.0 and the Profile version 2.0. Specifically, the Profile places the related supply chain risk management issues into its own function called "Extend" to make it easier for financial institutions to identify relevant third party risk management issues.

Profile users can easily find any deviations from NIST in the "NIST CSF v2 Mapping column" in the "CRI Profile v2.0 Structure" worksheet. For a summary of changes, see table 1 below.

Table 1: Summary of Changes between NIST CSF version 2 and CRI Profile version 2

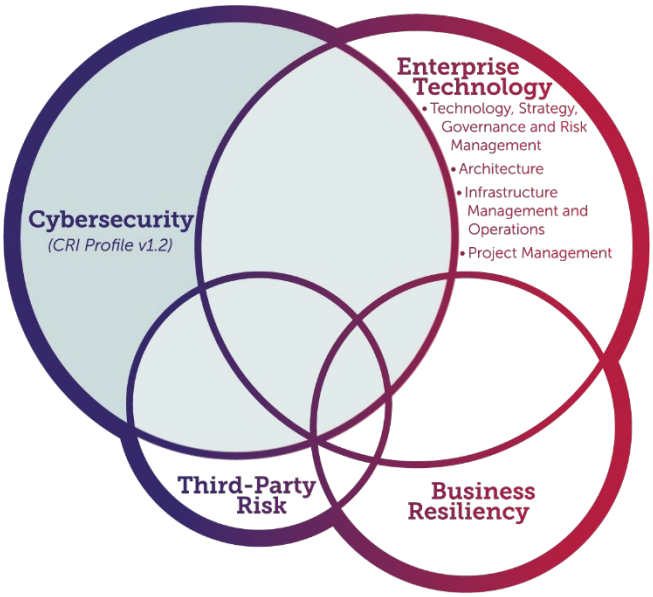
	GOVERN	IDENTIFY	PROTECT	DETECT	RESPOND	RECOVER	EXTEND
NIST CSF ver. 2							
Categories:	***6***	***3***	***5***	***2***	***4***	***2***	***--***
Subcategories:	***31***	***21***	***22***	***11***	***13***	***8***	***--***
CRI Profile ver. 2							
Categories:	***+ 2***	***same***	***same***	***same***	***same***	***same***	***+ 4***
Subcategories:	***+ 4***	***- 2***	***+ 1***	***same***	***same***	***same***	***+ 10***
Diagnostic Statements:	***97***	***64***	***74***	***24***	***16***	***11***	***32***

Moved to EXTEND

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.

2 Expanded Scope

Profile version 2.0 has been expanded to include enterprise technology, third-party risk management, and business continuity and resiliency, in addition to cybersecurity. This will assist financial institutions and examiners by reflecting the scope of typical regulatory examinations. In doing so, the Profile has revised existing language and added new topical areas, such as technology governance and encryption standards, to better reflect examinations.



Expanding the scope and coverage of the CRI Profile resulted in nearly all diagnostic statements being revised in some form. Organizations wishing to move from CRI Profile version 1.2.1 to version 2.0 should refer to the "Profile v1.2.1 Mapping" worksheet that provides additional detail on how each statement was revised. See table 2 below.

Table 2: Number of Diagnostic Statements by Impact Tier

Impact Tier	Profile version 1.2.1	Profile version 2.0
1	279	318
2	263	311
3	189	282
4	138	208

3 New Topics

CRI Profile version 2.0 includes roughly a dozen new control topics, including:

- Technology governance
- Technology architecture
- Operations, problem management, and IT service & support
- Project management
- Shadow IT management
- Cloud services access and authorization

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.

- Encryption standards & key management
- Time services
- Applications management
- Insider threat management
- Social media/dark web monitoring
- Procurement planning

4 Existing Topics Enhanced

CRI Profile version 2.0 provides additional coverage to the following topics, among others:

- Control testing and evaluation
- Exception management
- Asset lifecycle management
- Data governance and management
- Skill and resource assessment
- Business Impact Analyses
- Network device/firewall rule review
- Email verification mechanisms
- Secure SDLC
- Emergency changes
- Remote access devices (end points, mobile, virtual)
- Forensic investigations

5 New Features

Tagging

CRI Profile v2.0 now includes over 100 different subject tags, such as “threat intelligence” and “resilience.” Users can refer to the “Diagnostic Statement by Tag” and “Subject Tag List” worksheets in the Profile worksheet to find those most relevant to their needs.

Simplified Assessment Response Fields

It also includes assessment response fields that are more straightforward to assist users in more easily identifying relevant content and providing assessment rationales and supporting evidence.

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.

Response Summary

CRI Profile v2.0 now includes a summary of responses that indicates the distribution of responses by the Function, Category, or Subcategory level. This will provide organizations with the means to better visualize progress and identify gaps:

				Response Distribution								
			CRI Profile Total:	33	41	169	0	71	1	0	1	2
Outlin	Lev	Profile	Function / Category / Subcategory	Ye	No	Part	Yes-Risk Base	Yes-Compensating Control	Not Teste	I Don't Kno	To Be Assessed	Not Applica ble
001	F	GV	GOVERN	29	33	32	0	0	1	0	1	1
002	C	GV.OC	Organizational Context	7	2	3	0	0	0	0	1	1
008	C	GV.RM	Risk Management Strategy	16	4	5	0	0	1	0	0	0
018	C	GV.SC	Supply Chain Risk Management	6	1	0	0	0	0	0	0	0
029	C	GV.RR	Roles, Responsibilities, and Authorities	0	18	0	0	0	0	0	0	0
034	C	GV.PO	Policies, Processes, and Procedures	0	8	1	0	0	0	0	0	0
037	C	GV.OV	Oversight	0	0	7	0	0	0	0	0	0
041	C	GV.IR	Independent Risk Management Function	0	0	6	0	0	0	0	0	0
045	C	GV.AU	Independent Audit Function	0	0	10	0	0	0	0	0	0
049	F	ID	IDENTIFY	0	3	57	0	0	0	0	0	0
050	C	ID.AM	Asset Management	0	0	9	0	0	0	0	0	0
058	C	ID.RA	Risk Assessment	0	1	26	0	0	0	0	0	0
068	C	ID.IM	Improvement	0	2	22	0	0	0	0	0	0
073	F	PR	PROTECT	3	5	70	0	0	0	0	0	0
074	C	PR.AA	Identity Management, Authentication, and Access Control	0	0	13	0	0	0	0	0	0
081	C	PR.AT	Awareness and Training	0	0	12	0	0	0	0	0	0
084	C	PR.DS	Data Security	0	0	10	0	0	0	0	0	0
090	C	PR.PS	Platform Security	0	2	29	0	0	0	0	0	0
098	C	PR.IR	Technology Infrastructure Resilience	3	3	6	0	0	0	0	0	0
103	F	DE	DETECT	1	0	2	0	20	0	0	0	1
104	C	DE.CM	Continuous Monitoring	1	0	2	0	11	0	0	0	1
110	C	DE.AE	Adverse Event Analysis	0	0	0	0	9	0	0	0	0
117	F	RS	RESPOND	0	0	0	0	16	0	0	0	0
118	C	RS.MA	Incident Management	0	0	0	0	5	0	0	0	0
124	C	RS.AN	Incident Analysis	0	0	0	0	4	0	0	0	0
129	C	RS.CO	Incident Response Reporting and Communication	0	0	0	0	5	0	0	0	0
132	C	RS.MI	Incident Mitigation	0	0	0	0	2	0	0	0	0
135	F	RC	RECOVER	0	0	0	0	11	0	0	0	0
136	C	RC.RP	Incident Recovery Plan Execution	0	0	0	0	8	0	0	0	0
143	C	RC.CO	Incident Recovery Communication	0	0	0	0	3	0	0	0	0
146	F	EX	EXTEND	0	0	8	0	24	0	0	0	0
147	C	EX.DD	Procurement Planning and Due Diligence	0	0	0	0	12	0	0	0	0
152	C	EX.CN	Third-Party Contracts and Agreements	0	0	0	0	7	0	0	0	0
155	C	EX.MM	Monitoring and Managing Suppliers	0	0	4	0	5	0	0	0	0
158	C	EX.TR	Relationship Termination	0	0	4	0	0	0	0	0	0

6 New Mappings

The CRI Profile continues to connect key cybersecurity control principles to guidance from government agencies. For the most recent update, the Profile has been mapped to and integrated numerous global standards and supervisory expectations, including those from Japan, the European Union, Singapore, and the United States, among others. In doing so, the Profile allows financial institutions to assess themselves once, and offer as a compliance tool to multiple regulators.

Listed alphabetically below, specific mappings include:

- Department of Homeland Security's Cybersecurity and Infrastructure Security Agency's (CISA) Cross-Sector Cybersecurity Performance Goals 1.0.1 to the CRI Profile

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.

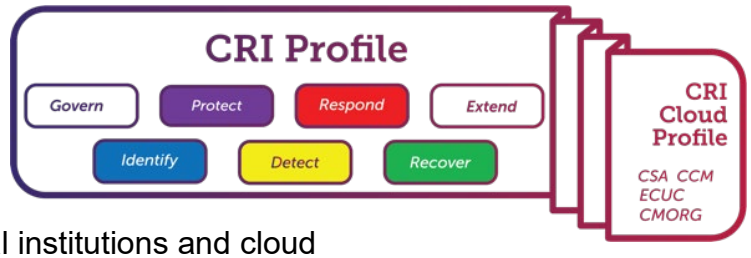
- European Banking Authority's (EBA) "Guidelines on ICT and Security Risk Management" to the CRI Profile
- European Central Bank, "Cyber resilience oversight expectations for financial market infrastructures" (CROE) (Dec 2018) to the CRI Profile
- The Federal Financial Institutions and Examination Council (FFIEC) Architecture, Instructure, and Operations Examination Handbook (June 2021) to the CRI Profile
- FFIEC Business Continuity Management Examination Handbook (November 2019) to the CRI Profile
- FFIEC Cybersecurity Assessment (CAT) Tool to the CRI Profile and CRI Profile to FFIEC CAT
- JFSA (Financial Services Agency, Japan) Comprehensive Guidelines for Supervision of Major Banks (June 2021) to the CRI Profile
- Monetary Authority of Singapore (MAS) Technology Risk Management Guidelines (Jan. 2021) and Cyber Hygiene Notice 655 to the CRI Profile
- New York State Department of Financial Services' (NYDFS) 23 NYCRR 500 Second Amendment to the CRI Profile
- NIST CSF version 2.0 to the CRI Profile (embedded in the "CRI Profile v2.0 Structure" worksheet).
- NIST Online Informative References (OLIR) for NIST CSF v2.0 and CRI Profile v2.0
- NIST Ransomware Profile to the CRI Profile
- Office of the Comptroller of the Currency (OCC) Cybersecurity Supervision Work Program References to the CRI Profile
- Securities and Exchange Commission's (SEC) Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure (August 2023) to the CRI Profile

7 Updated Guidebook

CRI Profile version 2.0 is accompanied with a revised Profile Guidebook (formerly the Profile Workbook) that includes detailed guidance on control objectives, as well as examples of effective evidence that could be used by financial institutions during examinations. The purpose of the Profile Guidebook is to (1) assist organizations in implementing the Profile and (2) drive consistency when completing the Profile within the financial sector. The Profile Guidebook provides interpretive guidance on each of the CRI Profile's 318 Diagnostic Statements and examples of effective evidence to support the organization's response. In this document, users can also find a listing of key terms and the full list of all 318 diagnostic statements and their corresponding impact tiers.

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.

8 Maintains Extensibility to Cloud



Like the prior version, CRI Profile version 2.0 remains extensible to other technology areas, such as cloud computing. In 2022, CRI published the Cloud Profile, which provides guidance to enable financial institutions and cloud service providers to come to contractual understanding more easily and should also facilitate more streamlined and secure processes for deploying cloud services.

In January 2023, the U.S. Department of the Treasury pointed to the CRI Cloud Profile as a resource for financial institutions to use for cloud implementation. Over the last year, CRI has been working with financial sector participants to update the Cloud Profile to mirror Profile version 2.0, enhance its functionality, and include additional global mappings.

The Cloud Profile v2.0 will include an updated mapping to the Cloud Security Alliance's Cloud Control Matrix and new mappings to the United Kingdom's Cross Market Operational Resilience Group's Cloud Control Framework and the European Cloud User Coalition's position paper. CRI anticipates publishing the Cloud Profile version 2.0 in the spring of 2024.

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.