Software Engineering Institute
Carnegie Mellon University

A Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR)

Jeffrey L. Pinckard
Michael Rattigan
Robert A. Vrtis

October 2016

TECHNICAL NOTE
CMU/SEI-2016-TN-008

Cybersecurity Assurance

http://www.sei.cmu.edu

REV-03.18.2016.0

This material is based upon work funded and supported by Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

This report was prepared for the
SEI Administrative Agent
AFLCMC/PZM
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

DM-0003949

Table of Contents

List of Figures

Executive Summary

This technical note describes the methodology we used and the observations we made while mapping the declarative statements found in the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the practice questions found in the US-CERT Cyber Resilience Review (CRR). This mapping enables financial organizations to use CRR results not only to gauge their cyber resilience, but to examine their current baseline with respect to the FFIEC CAT and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The mapping in this technical note is proposed by three senior engineers from the CERT Division of the Carnegie Mellon University Software Engineering Institute; these engineers are skilled in conducting CRRs and familiar with all practice questions and question guidance. Two also have the advantage of several years of experience in the financial sector. The team relied on their experience along with previous mappings of the CRR and FFIEC CAT to the NIST CSF to propose the mapping in this technical note.

The FFIEC published the CAT in June 2015 for financial institutions to use in assessing their cybersecurity readiness. The United States Department of Homeland Security (DHS) produced a similar assessment, the Cyber Resilience Review (CRR) version 2.0, in October 2011. The CRR is based on Carnegie Mellon University's CERT® Resilience Management Model (RMM) and is used by DHS in support of Presidential Policy Directive PPD-21 [WH 2013a] to encourage the adoption of the NIST CSF. While the CRR predates the establishment of the NIST CSF, the inherent principles and recommended practices within the CRR align closely with the central tenets of the CSF. Both the CAT and the CRR instruments map well to the NIST CSF. PPD-21 required NIST to create the CSF, and both documents support the implementation.

This technical note contains our mapping of declarative statements from the FFIEC CAT to the practice questions found in the CRR, a description of our approach, and our observations on mapping the CAT to CRR practices.

Abstract

This technical note describes the methodology we used and the observations we made while mapping the declarative statements found in the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the practice questions found in the Cyber Resilience Review (CRR). This mapping enables financial organizations to use CRR results not only to gauge their cyber resilience, but to examine their current baseline with respect to the FFIEC CAT and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The mapping in this technical note is proposed by three senior engineers from the CERT Division of the Carnegie Mellon University Software Engineering Institute; these engineers are skilled in conducting CRRs and familiar with all practice questions and question guidance. Two also have the advantage of several years of experience in the financial sector. The team relied on their experience along with previous mappings of the CRR and FFIEC CAT to the NIST CSF to propose the mapping in this technical note.

1 Background

1.1 What is the CRR?

The Cyber Resilience Review (CRR) is a no-cost, voluntary, non-technical assessment to evaluate operational resilience and cybersecurity capabilities within critical infrastructure and key resources sectors, as well as state, local, tribal, and territorial governments [US-CERT 2016].

The CRR establishes a baseline of cybersecurity capabilities, which helps an organization to understand its operational resilience. It also enables organizations to manage cyber risks to critical services during normal operations as well as during times of operational stress and crisis. The CRR is based on the CERT® Resilience Management Model (RMM) (http://www.cert.org/resilience/rmm.html), a process improvement model developed by Carnegie Mellon University's Software Engineering Institute (SEI) for managing operational resilience [SEI 2016].

The SEI CERT Division developed a crosswalk of the practices measured in the CRR to criteria of the specific outcomes articulated in the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). An organization can use the output of the CRR to approximate its conformance with the NIST CSF. Note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may either fall short of or exceed the corresponding practices and capabilities in the NIST CSF.

The CRR is a one-day, interview-based assessment of an organization's cybersecurity management program. It consists of 297 practice questions and is typically delivered in a six-hour workshop led by facilitators from the United States Department of Homeland Security (DHS). Using the CRR Self-Assessment package available from DHS, organizations can self-administer the CRR without needing the cybersecurity experts provided by DHS. The Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) contains 494 declarative statements and is also self-administered.

1.2 What is the NIST CSF?

The President issued Executive Order 13636, "Improving Critical Infrastructure Cybersecurity," on February 12, 2013, to better address cybersecurity risks [WH 2012b]. The Executive Order states, "…it is the policy of the United States to enhance the security and resilience of the Nation's critical infrastructure and to maintain a cyber environment that encourages efficiency, innovation, and economic prosperity while promoting safety, security, business confidentiality, privacy, and civil liberties." In enacting this policy, the Executive Order calls for the development of a voluntary, risk-based, cybersecurity framework—a set of industry standards and best practices to help organizations manage cybersecurity risks. The resulting framework was created through collaboration between NIST and the private sector. It uses a common language to address and manage cybersecurity risk in a cost-effective way based on business needs without placing additional regulatory requirements on businesses. The NIST CSF focuses on using business drivers to guide cybersecurity activities [NIST 2014].

The CSF consists of three parts: the Framework Core, the Framework Profile, and the Framework Implementation Tiers. The Framework Core is a set of cybersecurity activities, outcomes, and informative references that are common across critical infrastructure sectors, providing the detailed guidance for developing individual organizational Profiles. Through use of the Profiles, the CSF will help the

organization align its cybersecurity activities with its business requirements, risk tolerances, and resources. The Tiers provide a mechanism for organizations to view and understand the characteristics of their approach to managing cybersecurity risk.

The CSF enables organizations—regardless of size, degree of cybersecurity risk, or cybersecurity sophistication—to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure. The CSF provides organization and structure to today's multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today.

The Executive Order also directed sector-specific agencies to "review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments" [WH 2012b].

1.3 What is the FFIEC CAT?

The Federal Financial Institutions Examination Council (FFIEC) developed the Cybersecurity Assessment Tool (CAT) [FFIEC 2016a] on behalf of its members to help institutions identify risks and determine their cybersecurity preparedness. The CAT provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time. It incorporates cybersecurity-related principles from the FFIEC Information Technology (IT) Examination Handbook and regulatory guidance, and concepts from other industry standards and the NIST CSF.

The FFIEC Assessment has been mapped to the statements included in the NIST CSF. NIST reviewed and provided input on the mapping to ensure consistency with CSF principles and to highlight the complementary nature of the two resources.

1.4 What does this technical note provide?

This technical note describes the approach used to develop the crosswalk of the CRR practices to the FFIEC CAT declarative statements. Its goal is to help organizations within the financial services sector to use the CRR as an indicator of cybersecurity readiness. Both tools have been independently mapped to the NIST CSF; this technical note uses those independent mappings to map the CRR to the FFIEC CAT.

This technical note does the following:

- maps the FFIEC CAT declarative statements to CRR practice questions. This mapping highlights mutual coverage, provides supplemental guidance to practice questions when the question is not sufficiently specific, and identifies where gaps exist.
- explains the overlap between the CAT and CRR in terms of NIST CSF coverage
- highlights the differences by means of approach and by lack of mutual coverage
- discusses the value of the CRR to the financial sector

Other sector-specific agencies, such as the water sector and the electric sector, have developed their own tools; the methodology described here can be applied to develop additional mappings in a similar fashion.

2 Approach

The published mappings of both the CRR and the FFIEC CAT to the NIST CSF served as the initial baseline for our effort.

Starting with the CAT, we examined each declarative statement and the corresponding NIST CSF mapping to the CRR practices to determine if there was a functional match. This was accomplished by asking the following questions:

1. If the organization can claim the CAT's declarative statement was an accurate evaluation of the practices being performed, is it likely that the corresponding CRR practice question would be answered "Yes" based upon the question guidance provided for that practice?
2. Would other CRR practice questions also be answered "Yes"?
3. Should the CRR guidance be modified to reflect specific controls or concerns of the sector without changing the question?
4. Is there an adequate mapping to the CRR? If not, these statements were identified as gaps.

Roughly two-thirds of the FFIEC CAT declarative statements did not have corresponding NIST CSF mappings. The CAT is based on a number of declarative statements that address similar concepts across FFIEC-defined maturity levels. We used our interpretation of the CAT statement and examined the CRR questions and question guidance throughout all domains to identify the CRR questions which resulted in the most complete functional match with the NIST CSF mappings.

3 Relationship Between the Instruments RMM–CRR–CSF–FFIEC

3.1 CERT-RMM

First published in 2010, CERT-RMM is one of the first publications addressing the convergence of IT security, disaster recovery, and business continuity. It comprises 26 process areas that cover four areas of operational resilience management: Enterprise Management, Engineering, Operations, and Process Management. CERT-RMM is a full assessment vehicle offering fully proctored, documented assessments with associated certification that measures an organization's infrastructure and processes to successfully respond to disruption in a repeatable and organized way. Higher degrees of maturity produce more consistent, repeatable results. An organization's process maturity is measured by determining the degree to which key processes have been institutionalized. CERT-RMM depicts both staged and continuous representations of capability.

3.2 CRR

First published in 2011, the CRR is a derivative product of CERT-RMM built expressly for the U.S. Department of Homeland Security (DHS) as a lightweight assessment tool for critical infrastructure. It is intended as a one-day, facilitated instrument. The CRR narrowed the scope of examination from the 26 process areas that CERT-RMM associates with the full range of operational resilience to the 10 domains of practice that the CRR most closely associates with cybersecurity.

The CRR includes 269 questions that are extracted from CERT-RMM and organized into 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

Each domain is composed of a purpose statement, a set of specific goals and associated practice questions unique to the domain, and a standard set of Maturity Indicator Level (MIL) questions. The MIL questions are the same for each domain and examine the institutionalization of practices within an organization.

The CRR uses MILs to provide organizations with an approximation of the maturity of their practices in the 10 cybersecurity domains. In this approach, the organization's maturity is based on how completely the cybersecurity practices in each of the domains are institutionalized within the organization. Institutionalization means that cybersecurity practices become a deeper, more lasting part of the organization because they are managed and supported in meaningful ways. When cybersecurity practices become more institutionalized (or embedded), managers have more confidence in their predictability and reliability. The practices also are more likely to be sustained during times of disruption or stress to the organization.

The MIL scale itself uses six maturity levels, each with rigorous, defined components:

Incomplete → Performed → Planned → Managed → Measured → Defined

Figure 1: Maturity Levels in the CRR

MIL0: Incomplete—Practices in the domain are not being performed as measured by responses to the relevant CRR questions in the domain.

MIL1: Performed—All practices that support the goals in a domain are being performed as measured by responses to the relevant CRR questions.

MIL2: Planned—A specific practice in the CRR domain is not only performed but is also supported by planning, stakeholders, and relevant standards and guidelines.

MIL3: Managed—All practices in a domain are performed, are planned, and have the basic governance infrastructure in place to support the process.

MIL4: Measured—All practices in a domain are performed, planned, managed, monitored, and controlled.

MIL5: Defined—All practices in a domain are performed, planned, managed, measured, and consistent across all constituencies within an organization who have a vested interest in the performance of the practice.

In the above progression, an organization can only attain a given MIL if it has attained all lower MILs. In other words, an organization that fails to perform all of the cybersecurity practices at MIL1 in a domain would also fail to reach MIL2 in that domain, even if it has satisfied all the requirements at MIL2 performance of the practice.

3.3 FFIEC CAT

The financial industry's regulatory examination body (the FFIEC) published the CAT in 2015, answering the call to provide financial institutions with more direct guidance for navigating an increasingly complex cyber risk landscape. The FFIEC CAT incorporates cybersecurity-related principles from the FFIEC Information Technology (IT) Examination Handbook and regulatory guidance as well as concepts from the NIST CSF [FFIEC 2015a].

The FFIEC CAT is designed to help management assess their institution's cybersecurity preparedness, evaluate its cybersecurity preparedness alignment risks, and determine what risk management practices and controls are needed (or need enhancement) to achieve the desired state. It consists of two parts: Inherent Risk Profile and Cybersecurity Maturity. By completing both parts, management can evaluate whether the institution's inherent risk and preparedness are aligned.

- The **Inherent Risk Profile** contains descriptions of activities across risk categories with definitions for the lowest to highest levels of inherent risk. Inherent risk is the level of cybersecurity risk posed to the institution by technologies and connection types, delivery channels, online and mobile products and technology services, organizational characteristics, and external threats. It incorporates the type, volume, and complexity of the institution's operations as well as threats directed at the institution.
- **Cybersecurity Maturity** helps management measure the institution's level of risk and corresponding controls. The maturity levels range from "baseline" to "innovative." Cybersecurity maturity statements are made as to whether an institution's behaviors, practices, and processes can support cybersecurity preparedness within five domains [FFIEC 2015a].

Figure 2 shows the five domains defined in the FFIEC CAT and the assessment factors into which the declarative statements are grouped.

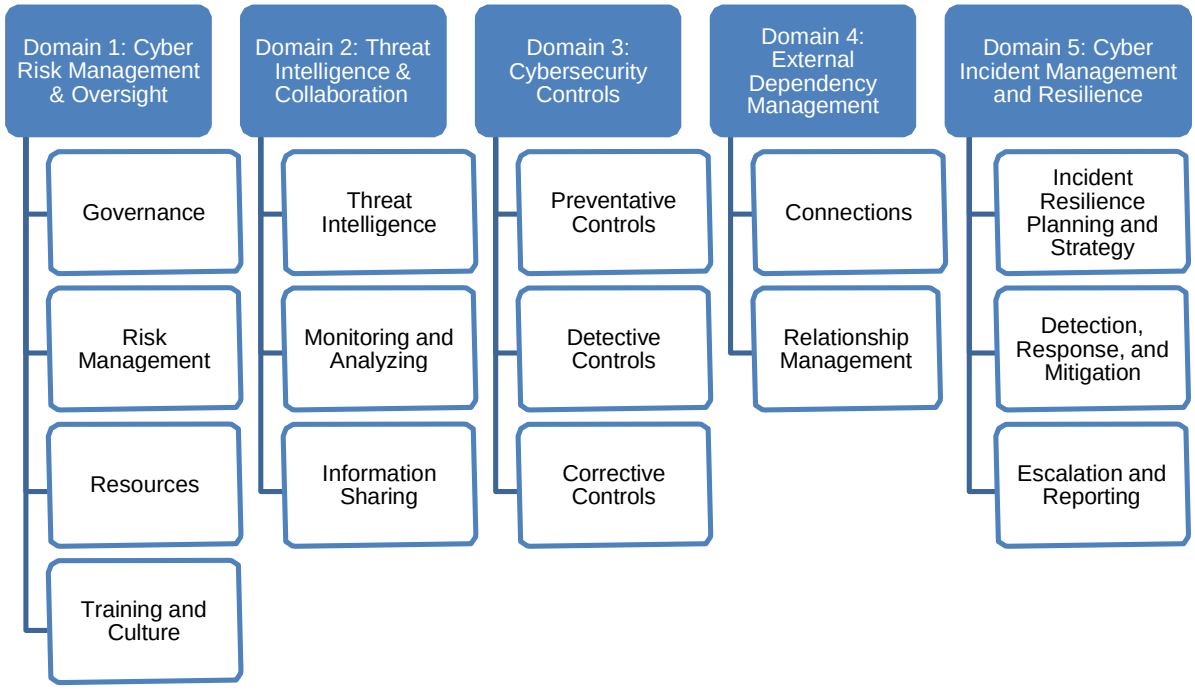

Figure 2: FFIEC CAT Domain Architecture

The domains include assessment factors and contributing components. Within each component, declarative statements describe activities supporting the assessment factor at each maturity level. Management determines which declarative statements best fit the current practices of the institution. **All declarative statements in each maturity level, and previous levels, must be attained and sustained to achieve that domain's maturity level.** While management can determine the institution's maturity level in each domain, the assessment is not designed to identify an overall cybersecurity maturity level. Instead, as an institution's inherent risk profile increases, its corresponding maturity level should increase.

Management can review the institution's Inherent Risk Profile in relation to its Cybersecurity Maturity results for each domain to understand whether they are aligned. The following table depicts the relationship between an institution's Inherent Risk Profile and its domain maturity levels, as there is no single expected level for an institution. In general, as inherent risk rises, an institution's maturity levels should also increase. An institution's Inherent Risk Profile and maturity levels will change over time as threats, vulnerabilities, and operational environments change.

Risk/ Maturity Relationship		Inherent Risk Levels				
		Least	Minimal	Moderate	Significant	Most
Cybersecurity Maturity Level for Each Domain	Innovative				■	■
	Advanced			■	■	■
	Intermediate		■	■	■	
	Evolving	■	■	■		
	Baseline	■	■			

Figure 3: Relationship of Maturity to Inherent Risk in the FFIEC CAT

This concept of maturity is different than the concept applied by the CRR. However, the mapping in this technical note considers all declarative statements at all maturity levels defined by the FFIEC CAT.

3.4 Difference in Maturity Modeling

The CRR and the FFIEC approach the issue of maturity differently. These differences result in some non-intuitive mappings of CRR maturity practices to FFIEC statements and of FFIEC maturity statements to CRR practices. Some declarative statements of maturity in the FFIEC may appear as basic practices in the CRR, and vice versa.

In general, we have observed that maturity models can be categorized using the following three types [Caralli 2013]:

- **progression models**, where increases in maturity levels indicate improvement of an attribute's maturity
- **capability models**, which describe the state of an organization's maturity relative to process maturity
- **hybrid models**, which combine the rigor of capability models and the ease of use and comprehensibility of progression models

The FFIEC CAT employs a hybrid maturity model.

Unlike the FFIEC CAT, the CRR more closely aligns with the capability maturity architecture of CERT-RMM. In this architecture, a core set of goals and practices—referred to as specific goals and practices in CERT-RMM—defines the basic knowledge and skills that must be demonstrated in the domain. The capability maturity dimension is represented by a generic set of goals and practices that indicate increasing levels of capability for performing the core set of goals and practices. Thus, in the CRR, the maturity dimension is singularly measured by the MIL scale. This explains a number of "gaps" in the mapping between the FFIEC CAT and the CRR that specifically apply to sector-level participation.

4 Correlation of the FFIEC Assessment and the CRR

Using the mappings of the CRR and FFIEC Assessment to the NIST CSF, we propose mapping the CRR practices to the FFIEC Assessment's Cybersecurity Maturity declarative statements according to the crosswalk shown in Appendix C.

The table in Appendix C uses the basic format found in the *FFIEC Cybersecurity Assessment Tool User's Guide* [FFIEC 2015b] and adds two columns: CRR Reference and Additions to CRR Question Guidance.

4.1 CRR Reference

The column labeled CRR Reference contains the mapping of the declarative statement to related CRR practice questions. In our judgment, if all CRR practice questions are answered "Yes," it is likely that the declarative statement would also be answered "Yes." In some cases, the CRR Reference also requires that guidance be added to the CRR question guidance to assist in interpreting the question in the context of an organization from the financial sector. The term "gap" is also found in this column. It indicates that the declarative statement does not have an equivalent practice in the CRR. When a gap is identified, a related CRR practice is also identified for consideration.

4.2 Additions to CRR Question Guidance

There are three possible entries in the Additions to CRR Question Guidance column.

- **Additional guidance** contains a specific statement that should be considered when answering the CRR practice question. It would therefore be added to the CRR Question Guidance found with the CRR data collection form.
- **Specific control** interprets the declarative statement as requiring that a specific control must be implemented and the declarative statement be addressed directly. The response to the CRR practice referenced is not considered to be sufficient.
- **Possibly related to …** provides a CRR practice question that relates to the declarative statement that the organization undergoing a CRR can use to interpret the results.

5 Assumptions

CRR Scoping/Critical Service selection is equal to the FFIEC Inherent Risk Profile exercise in the CAT.

6 Definitions

All definitions are from the *FFIEC IT Examination Handbook InfoBase Glossary* [FFIEC 2016b].

Cyber Event—A cybersecurity change or occurrence that may have an impact on organizational operations (including mission, capabilities, or reputation).

Cyber Incident—Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system or the information residing therein.

Cyber Resilience—The ability of a system or domain to withstand cyber attacks or failures, and in such events, to reestablish itself quickly.

Appendix A Executive Order—Improving Critical Infrastructure Cybersecurity

The following section of Executive Order 13636, Improving Critical Infrastructure Cybersecurity, established the CSF [WH 2013b].

Sec. 8. Voluntary Critical Infrastructure Cybersecurity Program. (a) The Secretary, in coordination with Sector-Specific Agencies, shall establish a voluntary program to support the adoption of the Cybersecurity Framework by owners and operators of critical infrastructure and any other interested entities (the "Program").

(b) Sector-Specific Agencies, in consultation with the Secretary and other interested agencies, shall coordinate with the Sector Coordinating Councils to review the Cybersecurity Framework and, if necessary, develop implementation guidance or supplemental materials to address sector-specific risks and operating environments.

Sec. 10. Adoption of Framework. (a) Agencies with responsibility for regulating the security of critical infrastructure shall engage in a consultative process with DHS, OMB, and the National Security Staff to review the preliminary Cybersecurity Framework and determine if current cybersecurity regulatory requirements are sufficient given current and projected risks. In making such determination, these agencies shall consider the identification of critical infrastructure required under section 9 of this order. Within 90 days of the publication of the preliminary Framework, these agencies shall submit a report to the President, through the Assistant to the President for Homeland Security and Counterterrorism, the Director of OMB, and the Assistant to the President for Economic Affairs, that states whether or not the agency has clear authority to establish requirements based upon the Cybersecurity Framework to sufficiently address current and projected cyber risks to critical infrastructure, the existing authorities identified, and any additional authority required.

(b) If current regulatory requirements are deemed to be insufficient, within 90 days of publication of the final Framework, agencies identified in subsection (a) of this section shall propose prioritized, risk-based, efficient, and coordinated actions, consistent with Executive Order 12866 of September 30, 1993 (Regulatory Planning and Review), Executive Order 13563 of January 18, 2011 (Improving Regulation and Regulatory Review), and Executive Order 13609 of May 1, 2012 (Promoting International Regulatory Cooperation), to mitigate cyber risk.

(c) Within 2 years after publication of the final Framework, consistent with Executive Order 13563 and Executive Order 13610 of May 10, 2012 (Identifying and Reducing Regulatory Burdens), agencies identified in subsection (a) of this section shall, in consultation with owners and operators of critical infrastructure, report to OMB on any critical infrastructure subject to ineffective, conflicting, or excessively burdensome cybersecurity requirements. This report shall describe efforts made by agencies, and make recommendations for further actions, to minimize or eliminate such requirements.

(d) The Secretary shall coordinate the provision of technical assistance to agencies identified in subsection (a) of this section on the development of their cybersecurity workforce and programs.

(e) Independent regulatory agencies with responsibility for regulating the security of critical infrastructure are encouraged to engage in a consultative process with the Secretary, relevant Sector-Specific Agencies,

and other affected parties to consider prioritized actions to mitigate cyber risks for critical infrastructure consistent with their authorities.

Sec. 11. Definitions. (a) "Agency" means any authority of the United States that is an "agency" under 44 U.S.C. 3502(1), other than those considered to be independent regulatory agencies, as defined in 44 U.S.C. 3502(5).

(b) "Critical Infrastructure Partnership Advisory Council" means the council established by DHS under 6 U.S.C. 451 to facilitate effective interaction and coordination of critical infrastructure protection activities among the Federal Government; the private sector; and State, local, territorial, and tribal governments.

(c) "Fair Information Practice Principles" means the eight principles set forth in Appendix A of the National Strategy for Trusted Identities in Cyberspace.

(d) "Independent regulatory agency" has the meaning given the term in 44 U.S.C. 3502(5).

(e) "Sector Coordinating Council" means a private sector coordinating council composed of representatives of owners and operators within a particular sector of critical infrastructure established by the National Infrastructure Protection Plan or any successor.

(f) "Sector-Specific Agency" has the meaning given the term in Presidential Policy Directive-21 of February 12, 2013 (Critical Infrastructure Security and Resilience), or any successor.

Sec. 12. General Provisions. (a) This order shall be implemented consistent with applicable law and subject to the availability of appropriations. Nothing in this order shall be construed to provide an agency with authority for regulating the security of critical infrastructure in addition to or to a greater extent than the authority the agency has under existing law. Nothing in this order shall be construed to alter or limit any authority or responsibility of an agency under existing law.

(b) Nothing in this order shall be construed to impair or otherwise affect the functions of the Director of OMB relating to budgetary, administrative, or legislative proposals.

(c) All actions taken pursuant to this order shall be consistent with requirements and authorities to protect intelligence and law enforcement sources and methods. Nothing in this order shall be interpreted to supersede measures established under authority of law to protect the security and integrity of specific activities and associations that are in direct support of intelligence and law enforcement operations.

(d) This order shall be implemented consistent with U.S. international obligations.

(e) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

Appendix B Types of Maturity Models

Maturity models can be categorized as progression models, capability models, or a combination of the two (hybrid models). Hybrid models provide the rigor of capability maturity models while embracing the ease of use and comprehensibility of progression models [Caralli 2013]. One example of a hybrid model is the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) [DOE 2016], which was developed by applying the capability maturity concepts in CERT-RMM to existing codes of practice in the energy sector. ES-C2M2 also incorporates an enhanced maturity scaling.

The Cyber Resilience Review (CRR) is a lightweight assessment method derived from CERT-RMM version 1.1. It was created in collaboration with the Department of Homeland Security for the purpose of evaluating the cybersecurity and service continuity practices of critical infrastructure owners and operators. The CRR questionnaire, containing 269 questions, is delivered in a six-hour facilitated workshop setting. Answers are elicited from cybersecurity, operations, physical security, and business continuity personnel within critical infrastructure organizations. The CRR has been used to examine more than 200 organizations within 12 of the 16 critical infrastructure sectors.

CRR Architecture

The CRR comprises 42 goals and 139 specific practices extracted from CERT-RMM and organized in 10 domains:

1. Asset Management
2. Controls Management
3. Configuration and Change Management
4. Vulnerability Management
5. Incident Management
6. Service Continuity Management
7. Risk Management
8. External Dependencies Management
9. Training and Awareness
10. Situational Awareness

The length and pace of the CRR did not permit an adequate evaluation of practices at MIL6 (Shared). This explains a number of gaps in the FFIEC CAT > CRR Mapping.

Unlike ES-C2M2, which deploys a hybrid architecture to measure domain progress and capability maturity, the CRR more closely aligns with the capability maturity architecture of CERT-RMM. In this architecture, a core set of goals and practices—referred to as specific goals and practices in CERT-RMM—defines the basic knowledge and skills that must be demonstrated in the domain. The capability maturity dimension is represented by a generic set of goals and practices that indicate increasing levels of capability for performing the core set of goals and practices. Thus, in the CRR, the maturity dimension is singularly measured by the MIL scale.

If the previous conditions are met, the organization is said to be achieving the domain in a performed state. The practices that define the domain are observable, but no determination can be made about the degree to which these practices are

- repeatable under varying conditions
- consistently applied
- able to produce predictable and acceptable outcomes
- retained during times of stress

To test for these conditions, a common set of 13 MIL questions is applied to the domain—but only after MIL1 is achieved. MILs are cumulative; to achieve a MIL in a specific domain, an organization must perform all of the practices in that level and in the preceding MILs. For example, an organization must perform all of the domain practices in both MIL1 and MIL2 to achieve MIL2 in the domain.

Appendix C FFIEC CAT to CRR Mapping

This appendix contains a mapping (or crosswalk) between the Cyber Resilience Review (CRR) and the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT). This mapping was developed by members of the CERT Division of the Software Engineering Institute and could be used to inform a discussion with the developers of the FFIEC CAT.

Cyber Resilience Review (CRR)

The CRR was developed with the Department of Homeland Security (DHS) Office of Cybersecurity and Communications as a no-cost, non-technical assessment of an organization's operational resilience and cybersecurity capabilities. The goal of the CRR is to develop an understanding of an organization's ability to adapt to rapidly changing conditions and how well it manages the risk of disruption to its critical information technology services during both normal operation and times of operational stress and crisis.

The CERT Division has developed a correlation of the practices measured in the CRR to criteria of the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). An organization can use the output of the CRR to approximate its conformance with the NIST CSF. It is important to note that the CRR and NIST CSF are based on different catalogs of practice. As a result, an organization's fulfillment of CRR practices and capabilities may either fall short of or exceed the corresponding practices and capabilities in the NIST CSF.

FFIEC Cybersecurity Assessment Tool (CAT)

The FFIEC developed the CAT on behalf of its members. The FFIEC CAT helps financial institutions to identify their risks and determine their cybersecurity preparedness. It provides a repeatable and measurable process for institutions to measure their cybersecurity preparedness over time.

The FFIEC CAT has been mapped to the statements included in the NIST CSF. NIST reviewed and provided input on the mapping to ensure consistency with CSF principles and to highlight the complementary nature of the two resources.

Correlation of the FFIEC CAT and the CRR

Using the mappings of the CRR and FFIEC CAT to the NIST CSF, we have completed and propose the following mapping of the CRR practices to the Cybersecurity Maturity declarative statements in the FFIEC CAT.

The crosswalk table in this appendix uses the basic format found in the *FFIEC Cybersecurity Assessment Tool User's Guide* [FFIEC 2015b] and adds two columns: CRR Reference and Additions to CRR Question Guidance.

CRR Reference

The column labeled CRR Reference contains the proposed mapping of the declarative statement to related CRR practice questions. In our judgment, if all CRR practice questions are answered "Yes," it is likely that the declarative statement would also be answered "Yes." In some cases, the CRR Reference also requires that guidance be added to the CRR question guidance to assist in interpreting the question in the context of

an organization from the financial sector. The term “Gap” indicates that the declarative statement does not have an equivalent practice in the CRR.

Additions to CRR Question Guidance

There are three possible entries in the Additions to CRR Question Guidance column.

Additional guidance contains a specific statement that should be considered when answering the CRR practice question and would therefore be added to the CRR Question Guidance found with the CRR data collection form.

Specific control interprets the declarative statement as requiring that a specific control must be implemented and the declarative statement be addressed directly. The response to the CRR practice referenced is not considered sufficient.

Possibly related to… provides a CRR practice question that relates to the declarative statement that the organization undergoing a CRR can use to interpret the results.

FFIEC CAT > CRR Crosswalk

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Domain 1: Cyber Risk Management and Oversight				
Assessment Factor: Governance				
OVERSIGHT	Baseline	MIL3.Q4 – all MIL4.Q1 – all MIL4.Q2 – all MIL4.Q3 – all AM:MIL4.Q1 AM:MIL4.Q2 AM:MIL4.Q3 SCM:MIL4.Q1 SCM:MIL4.Q2 SCM:MIL4.Q3	Designated members of management are held accountable by the board or an appropriate board committee for implementing and managing the information security and business continuity programs. (FFIEC Information Security Booklet, page 3)	
		RM:G3.Q1 RM:G4.Q1	Information security risks are discussed in management meetings when prompted by highly visible cyber events or regulatory alerts. (FFIEC Information Security Booklet, page 6)	
		MIL3.Q4 – all MIL4.Q1 – all MIL4.Q2 – all MIL4.Q3 – all	Management provides a written report on the overall status of the information security and business continuity programs to the board or an appropriate board committee at least annually. (FFIEC Information Security Booklet, page 5)	
		MIL3.Q3 – all	The budgeting process includes information security related expenses and tools. (FFIEC E-Banking Booklet, page 20)	
		EDM:G2.Q1 EDM:G5.Q2	Management considers the risks posed by other critical infrastructures (e.g., telecommunications, energy) to the institution. (FFIEC Business Continuity Planning Booklet, page J-12)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Evolving	MIL3.Q4 – all MIL4.Q1 – all MIL4.Q2 – all MIL4.Q3 – all	At least annually, the board or an appropriate board committee reviews and approves the institution's cybersecurity program.	
		AM:G3.Q2 CM:G1.Q1 CM:G2.Q1 IM:G2.Q8 IM:G2.Q9 IM:MIL3.Q1	Management is responsible for ensuring compliance with legal and regulatory requirements related to cybersecurity.	
		MIL3.Q2 – all MIL3.Q3 – all	Cybersecurity tools and staff are requested through the budget process.	
		IM:G5.Q2	There is a process to formally discuss and estimate potential expenses associated with cybersecurity incidents as part of the budgeting process.	Additional guidance—FFIEC requires that there is a specific link between the incident management process and the budget process.
	Intermediate	TA:G2.Q6 MIL2.Q3 – all MIL4.Q3 – all	The board or an appropriate board committee has cybersecurity expertise or engages experts to assist with oversight responsibilities.	Additional guidance—FFIEC requires specifically that the board have cybersecurity expertise available.
		SA:MIL4.Q3	The standard board meeting package includes reports and metrics that go beyond events and incidents to address threat intelligence trends and the institution's security posture.	
		RM:G2.Q3 RM:G2.Q4 RM:MIL5.Q1	The institution has a cyber risk appetite statement approved by the board or an appropriate board committee.	Additional guidance—FFIEC requires that cyber risk appetite statement is approved by the board.
		RM:G2.Q4 RM:G4.Q2	Cyber risks that exceed the risk appetite are escalated to management.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		MIL4.Q1 – all MIL4.Q2 – all MIL4.Q3 – all	The board or an appropriate board committee ensures management's annual cybersecurity self-assessment evaluates the institution's ability to meet its cyber risk management standards.	
	Advanced	RM:MIL3.Q1	The board or an appropriate board committee reviews and approves management's prioritization and resource allocation decisions based on the results of the cyber assessments.	Additional guidance—FFIEC requires board approval of management activity.
		RM:MIL3.Q4	The board or an appropriate board committee ensures management takes appropriate actions to address changing cyber risks or significant cybersecurity issues.	Additional guidance—FFIEC requires the board to review risk management activities.
		RM:MIL2.Q1 RM:Mil3.Q3	The budget process for requesting additional cybersecurity staff and tools is integrated into business units' budget processes.	
		RM:G2.Q4 RM:MIL5.Q1	The board- or board-committee-approved cyber risk appetite statement is part of the enterprise-wide risk appetite statement.	Additional guidance—FFIEC states that risk tolerance parameters define risk appetite.
		MIL4.Q1 – all MIL4.Q2 – all MIL4.Q3 – all RM:MIL5.Q2	Management has a formal process to continuously improve cybersecurity oversight.	Additional guidance for RM:MIL5.Q2—FFIEC requires continuous improvement of cybersecurity oversight.
		VM:G1.Q1 VM:G1.Q2 VM:G1.Q3 VM:G1.Q4 VM:G1.Q5	The budget process for requesting additional cybersecurity staff and tools maps current resources and tools to the cybersecurity strategy.	
		RM:MIL4.Q1	Management and the board or an appropriate board committee hold business units accountable for effectively managing all cyber risks associated with their activities.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		IM:G5.Q1 IM:G5.Q2	Management identifies root cause(s) when cyber attacks result in material loss.	
		MIL4.Q1 – all	The board or an appropriate board committee ensures that management's actions consider the cyber risks that the institution poses to the financial sector.	
	Innovative	MIL5.Q2 – all	The board or an appropriate board committee discusses ways for management to develop cybersecurity improvements that may be adopted sector-wide.	
		MIL4.Q1 – all	The board or an appropriate board committee verifies that management's actions consider the cyber risks that the institution poses to other critical infrastructures (e.g., telecommunications, energy).	
STRATEGY/POLICIES	Baseline	RM:G1.Q3	The institution has an information security strategy that integrates technology, policies, procedures, and training to mitigate risk. (FFIEC Information Security Booklet, page 3)	
		RM:MIL2.Q2	The institution has policies commensurate with its risk and complexity that address the concepts of information technology risk management. (FFIEC Information Security Booklet, page, 16)	
		SA:G3.Q2 SA:MIL2.Q2 SA:MIL2.Q4	The institution has policies commensurate with its risk and complexity that address the concepts of threat information sharing. (FFIEC EBanking Booklet, page 28)	
		RM:G5.Q1 MIL2.Q2 – all	The institution has board-approved policies commensurate with its risk and complexity that address information security. (FFIEC Information Security Booklet, page 16)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		EDM:MIL2.Q2	The institution has policies commensurate with its risk and complexity that address the concepts of external dependency or third-party management. (FFIEC Outsourcing Booklet, page 2)	
		IM:MIL2.Q2	The institution has policies commensurate with its risk and complexity that address the concepts of incident response and resilience. (FFIEC Information Security Booklet, page 83)	
		MIL5:Q1 – all	All elements of the information security program are coordinated enterprise-wide. (FFIEC Information Security Booklet, page 7)	
	Evolving	RM:G1.Q3	The institution augmented its information security strategy to incorporate cybersecurity and resilience.	
		MIL2:Q4 – all	The institution has a formal cybersecurity program that is based on technology and security industry standards or benchmarks.	
		CCM:MIL2.Q2 RM:MIL4.Q1 RM:MIL4.Q2	A formal process is in place to update policies as the institution's inherent risk profile changes.	Additional guidance for CCM:MIL2.Q2—FFIEC requires that a formal process to change policies is included in the Change Management policy.
	Intermediate	SA:MIL2.Q2	The institution has a comprehensive set of policies commensurate with its risk and complexity that address the concepts of threat intelligence.	
		MIL4.Q1 – all	Management periodically reviews the cybersecurity strategy to address evolving cyber threats and changes to the institution's inherent risk profile.	
		AM:G1.Q4 MIL3:Q4 – all	The cybersecurity strategy is incorporated into, or conceptually fits within, the institution's enterprise-wide risk management strategy.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		MIL2.Q1 – all MIL3:Q1 – all MIL4.Q1 – all MIL4.Q2 – all	Management links strategic cybersecurity objectives to tactical goals.	
		MIL5.Q1 – all	A formal process is in place to cross-reference and simultaneously update all policies related to cyber risks across business lines.	
	Advanced	MIL2.Q1 – all	The cybersecurity strategy outlines the institution's future state of cybersecurity with short-term and long-term perspectives.	
		MIL2.Q4 – all	Industry-recognized cybersecurity standards are used as sources during the analysis of cybersecurity program gaps.	
		AM:G1.Q3	The cybersecurity strategy identifies and communicates the institution's role as a component of critical infrastructure in the financial services industry.	
		AM:G1.Q3 RM:G2.Q3 RM:G2.Q4	The risk appetite is informed by the institution's role in critical infrastructure.	
		MIL5.Q2 – all	Management is continuously improving the existing cybersecurity program to adapt as the desired cybersecurity target state changes.	
	Innovative	AM:G1.Q3	The cybersecurity strategy identifies and communicates the institution's role as it relates to other critical infrastructures.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
IT ASSET MANAGEMENT	Baseline	AM:G2.Q1	An inventory of organizational assets (e.g., hardware, software, data, and systems hosted externally) is maintained. (FFIEC Information Security Booklet, page 9)	
		AM:G3.Q1 AM:G7.Q1 AM:G7.Q2	Organizational assets (e.g., hardware, systems, data, and applications) are prioritized for protection based on the data classification and business value. (FFIEC Information Security Booklet, page 12)	
		AM:MIL2.Q2 AM:MIL3.Q2	Management assigns accountability for maintaining an inventory of organizational assets. (FFIEC Information Security Booklet, page 9)	
		CCM:G1.Q1	A change management process is in place to request and approve changes to systems configurations, hardware, software, applications, and security tools. (FFIEC Information Security Booklet, page 56)	
	Evolving	AM:G4.Q2 AM:MIL4.Q1	The asset inventory, including identification of critical assets, is updated at least annually to address new, relocated, re-purposed, and sunset assets.	
		CCM:G1.Q2 CCM:G1.Q6	The institution has a documented asset life-cycle process that considers whether assets to be acquired have appropriate security safeguards.	
		AM:G6:Q6	The institution proactively manages system end of life (EOL) (e.g., replacement) to limit security risks.	Additional guidance—FFIEC requires asset management must be specific to a system's EOL.
		CCM:G1.Q1 CCM:MIL3.Q2	Changes are formally approved by an individual or committee with appropriate authority and with separation of duties.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Intermediate	CCM:G3.Q2	Baseline configurations cannot be altered without a formal change request, documented approval, and an assessment of security implications.	
		CCM:G1.Q1	A formal IT change management process requires cybersecurity risk to be evaluated during the analysis, approval, testing, and reporting of changes.	Additional guidance—FFIEC requires that cybersecurity risks must be evaluated as part of the change management process.
	Advanced	CCM:G1.Q2 RM:G1.Q1 RM:G2.Q1	Supply chain risk is reviewed before the acquisition of mission-critical information systems including system components.	Additional guidance—FFIEC requires that supply chain risk should be explicitly included.
		AM:MIL4.Q1	Automated tools enable tracking, updating, asset prioritizing, and custom reporting of the asset inventory.	Additional guidance—FFIEC requires that automated reporting is required.
		CCM:G2.Q2	Automated processes are in place to detect and block unauthorized changes to software and hardware.	Additional guidance—FFIEC requires automated detection of unauthorized changes to software and hardware.
		CCM:G1.Q2 RM:G4.Q1	The change management system uses thresholds to determine when a risk assessment of the impact of the change is required.	
	Innovative	RM:G2.Q3	A formal change management function governs decentralized or highly distributed change requests and identifies and measures security risks that may cause increased exposure to cyber attack.	Additional guidance—FFIEC requires that risk tolerances should specifically address decentralized and highly distributed systems.
		CCM:G2.Q2 CCM:MIL5.Q1	Comprehensive automated enterprise tools are implemented to detect and block unauthorized changes to software and hardware.	Additional guidance—FFIEC requires automated detection and blocking of unauthorized changes.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Assessment Factor: Risk Management				
RISK MANAGEMENT	Baseline	SCM:G1.Q3	An information security and business continuity risk management function(s) exists within the institution. (FFIEC Information Security Booklet, page 68)	
	Evolving	RISK:G1.Q1 RISK:G1.Q2 RISK:G1.Q3	The risk management program incorporates cyber risk identification, measurement, mitigation, monitoring, and reporting.	
		CCM:G4.Q1	Management reviews and uses the results of audits to improve existing cybersecurity policies, procedures, and controls.	
		RISK:G5.Q2	Management monitors moderate and high residual risk issues from the cybersecurity risk assessment until items are addressed.	
	Intermediate	MIL3:Q1 – all	The cybersecurity function has a clear reporting line that does not present a conflict of interest.	Additional guidance—FFIEC requires that management activities do not present a conflict of interest.
		RM:G2.Q1	The risk management program specifically addresses cyber risks beyond the boundaries of the technological impacts (e.g., financial, strategic, regulatory, compliance).	
		MIL4:Q1 – all	Benchmarks or target performance metrics have been established for showing improvements or regressions of the security posture over time.	
		VM:G3.Q1	Management uses the results of independent audits and reviews to improve cybersecurity.	
		RM:G4.Q1	There is a process to analyze and assign potential losses and related expenses, by cost center, associated with cybersecurity incidents.	Additional guidance—FFIEC requires that operational risk should be related to the organization's financial management practice.
	Advanced	MIL 3.Q2 – all MIL 4.Q1 – all MIL 4.Q2 – all MIL 4.Q3 – all	Cybersecurity metrics are used to facilitate strategic decision making and funding in areas of need.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		RM:G2.Q3	Independent risk management sets and monitors cyber-related risk limits for business units.	Additional guidance—FFIEC requires that independent risk management establishes risk tolerance parameters.
		RM:MIL4.Q1 RM: MIL4.Q2 RM: MIL4.Q3	Independent risk management staff escalates to management and the board or an appropriate board committee significant discrepancies from business unit's assessments of cyber-related risk.	Additional guidance—FFIEC requires independent risk management staff to report risk management activities to the board.
		IM:G5.Q2	A process is in place to analyze the financial impact cyber incidents have on the institution's capital.	Additional guidance—FFIEC requires a link to Financial Risk Management Process.
		IM:G2.Q1 IM:G2.Q2 IM:G2.Q3 IM:G2.Q4 IM:G2.Q5 MIL 4.Q2 – all	The cyber risk data aggregation and real-time reporting capabilities support the institution's ongoing reporting needs, particularly during cyber incidents.	Additional guidance—FFIEC requires real-time reporting for incident management.
	Innovative	RM:G1.Q3 IM:G2.Q4	The risk management function identifies and analyzes commonalities in cyber events that occur both at the institution and across other sectors to enable more predictive risk management.	
		AM:G1.Q3 RM:G2.Q1 RM:G2.Q2 RM:G2.Q3	A process is in place to analyze the financial impact that a cyber incident at the institution may have across the financial sector.	Additional guidance—FFIEC requires that financial impacts should take into account potential sector impacts.
RISK ASSESSMENT	Baseline	RM:G2.Q1 RM:G2.Q3	A risk assessment focused on safeguarding customer information identifies reasonable and foreseeable internal and external threats, the likelihood and potential damage of threats, and the sufficiency of policies, procedures, and customer information systems. (FFIEC Information Security Booklet, page 8)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CM:G1.Q1 RM:G5.Q1	The risk assessment identifies internet-based systems and high-risk transactions that warrant additional authentication controls. (FFIEC Information Security Booklet, page 12)	
		CCM:G2.Q7	The risk assessment is updated to address new technologies, products, services, and connections before deployment. (FFIEC Information Security Booklet, page 13)	
	Evolving	CCM:G1.Q1 CCM:G1.Q2 EDM:G2.Q1 VM:G3.Q1 RM:G1.Q3	Risk assessments are used to identify the cybersecurity risks stemming from new products, services, or relationships.	
		RM:G2.Q1 RM:G2.Q3 VM:G2.Q1 SA:G1.Q2 VM:G2.Q3	The focus of the risk assessment has expanded beyond customer information to address all information assets.	
		RM:G1.Q1 RM:G2.Q1	The risk assessment considers the risk of using EOL software and hardware components.	Additional guidance—FFIEC requires that risk assessments must explicitly consider EOL as a risk source and impact area.
	Intermediate	RM:MIL2.Q4	The risk assessment is adjusted to consider widely known risks or risk management practices.	
	Advanced	RM:MIL2.Q1 RM:MIL2.Q2 RM:MIL5.Q1	An enterprise-wide risk management function incorporates cyber threat analysis and specific risk exposure as part of the enterprise risk assessment.	
	Innovative	VM:G3.Q2	The risk assessment is updated in real time as changes to the risk profile occur, new applicable standards are released or updated, and new exposures are anticipated.	Additional guidance—FFIEC requires that risk assessments are updated in real time.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		VM:G3.Q2	The institution uses information from risk assessments to predict threats and drive real-time responses.	
		VM:G1.Q2	Advanced or automated analytics offer predictive information and real-time risk metrics.	
AUDIT	Baseline	RM:MIL3.Q4 RM:MIL4.Q1	Independent audit or review evaluates policies, procedures, and controls across the institution for significant risks and control issues associated with the institution's operations, including risks in new products, emerging technologies, and information systems. (FFIEC Audit Booklet, page 4)	Additional guidance—Note: The FFIEC refers to "independent audits" throughout while the CRR refers to these as "external audits."
		CM:G3.Q1	The independent audit function validates controls related to the storage or transmission of confidential data. (FFIEC Audit Booklet, page 1)	
		CM:G4.Q1	Logging practices are independently reviewed periodically to ensure appropriate log management (e.g., access controls, retention, and maintenance). (FFIEC Operations Booklet, page 29)	
		CM:G4.Q2	Issues and corrective actions from internal audits and independent testing/assessments are formally tracked to ensure procedures and control lapses are resolved in a timely manner. (FFIEC Information Security Booklet, page 6)	
	Evolving	RM:G2.Q3 RM:MIL3.Q4	The independent audit function validates that the risk management function is commensurate with the institution's risk and complexity.	
		SA:MIL3.Q4	The independent audit function validates that the institution's threat information sharing is commensurate with the institution's risk and complexity.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CM:MIL3.Q4	The independent audit function validates that the institution's cybersecurity controls function is commensurate with the institution's risk and complexity.	
		EDM:MIL3.Q4	The independent audit function validates that the institution's third-party relationship management is commensurate with the institution's risk and complexity.	
		IM:MIL3.Q4	The independent audit function validates that the institution's incident response program and resilience are commensurate with the institution's risk and complexity.	
	Intermediate	RM:MIL2.Q1	A formal process is in place for the independent audit function to update its procedures based on changes to the institution's inherent risk profile.	Additional guidance—FFIEC requires the organization establish an independent audit function as part of its risk management plan.
		SA:MIL3.Q4	The independent audit function validates that the institution's threat intelligence and collaboration are commensurate with the institution's risk and complexity.	
		RM:G2.Q4 RM:MIL4.Q1	The independent audit function regularly reviews management's cyber risk appetite statement.	Additional guidance—FFIEC requires that risk tolerance thresholds need to be reviewed by independent audit on a regular basis.
		TA:G1.Q3 TA:MIL4.Q1	Independent audits or reviews are used to identify gaps in existing security capabilities and expertise.	Additional guidance—FFIEC requires that reviews are conducted by independent audits.
	Advanced	RM:MIL2.Q1	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across the sector.	Additional guidance—FFIEC requires that the independent audit function defined in the Risk Management plan updates its procedures based on changes to the threat landscape.
		RM:G2.Q4 RM:MIL4.Q1	The independent audit function regularly reviews the institution's cyber risk appetite statement in comparison to assessment results and incorporates gaps into the audit strategy.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		RM:G4.Q1 RM:G4.Q2	Independent audits or reviews are used to identify cybersecurity weaknesses, root causes, and the potential impact to business units.	
	Innovative	SA:G2.Q2 RM:G1.Q3 RM:MIL3.Q1	A formal process is in place for the independent audit function to update its procedures based on changes to the evolving threat landscape across other sectors the institution depends upon.	
		CM:MIL2.Q4	The independent audit function uses sophisticated data mining tools to perform continuous monitoring of cybersecurity processes or controls.	Additional guidance—FFIEC requires that standards and guidelines support the selection and acquisition of tools used in continuous monitoring.
Assessment Factor: Resources				
STAFFING	Baseline	AM:MIL2.Q3 CM:MIL2.Q3	Information security roles and responsibilities have been identified. (FFIEC Information Security Booklet, page 7)	
		TA:G1.Q3	Processes are in place to identify additional expertise needed to improve information security defenses. (FFIEC Information Security Work Program, Objective I: 2-8)	
	Evolving	MIL2.Q4 – all MIL3.Q2 – all MIL3.Q3 – all	A formal process is used to identify cybersecurity tools and expertise that may be needed.	
		MIL3:Q1 – all MIL3:Q2 – all	Management with appropriate knowledge and experience leads the institution's cybersecurity efforts.	
		TA:G2.Q2 SA:G1.Q3 SA:G3.Q3	Staff with cybersecurity responsibilities have the requisite qualifications to perform the necessary tasks of the position.	
		AM:G5.Q1 CM:G2.Q9CC M:G2.Q4	Employment candidates, contractors, and third parties are subject to background verification proportional to the confidentiality of the data accessed, business requirements, and acceptable risk.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Intermediate	Gap	The institution has a program for talent recruitment, retention, and succession planning for the cybersecurity and resilience staffs.	
	Advanced	Gap	The institution benchmarks its cybersecurity staffing against peers to identify whether its recruitment, retention, and succession planning are commensurate.	
		Gap	Dedicated cybersecurity staff develops, or contributes to developing, integrated enterprise-level security and cyber defense strategies.	
	Innovative	Gap	The institution actively partners with industry associations and academia to inform curricula based on future cybersecurity staffing needs of the industry.	
Assessment Factor: Training and Culture				
TRAINING	Baseline	TA:G2.Q1 TA:G2.Q2	Annual information security training is provided. (FFIEC Information Security Booklet, page 66)	
		TA:G1.Q1 TA:G1.Q4 TA:G2.Q1 TA:G2.Q2	Annual information security training includes incident response, current cyber threats (e.g., phishing, spear phishing, social engineering, and mobile security), and emerging issues. (FFIEC Information Security Booklet, page 66)	
		SA:G2.Q1 SA:G3.Q1	Situational awareness materials are made available to employees when prompted by highly visible cyber events or by regulatory alerts. (FFIEC Information Security Booklet, page 7)	
		TA:G1.Q1 TA:G2.Q1	Customer awareness materials are readily available (e.g., DHS Cybersecurity Awareness Month materials). (FFIEC E-Banking Work Program, Objective 6-3)	Additional guidance—FFIEC requires that awareness materials are provided to customers.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Evolving	TA:G1.Q4 TA:G2.Q2 TA:MIL3.Q3	The institution has a program for continuing cybersecurity training and skill development for cybersecurity staff.	
		TA:G2.Q6	Management is provided cybersecurity training relevant to their job responsibilities.	
		TA:G2.Q5 TA:G2.Q7	Employees with privileged account permissions receive additional cybersecurity training commensurate with their levels of responsibility.	
		TA:G2.Q2	Business units are provided cybersecurity training relevant to their particular business risks.	
		TA:G2.Q3	The institution validates the effectiveness of training (e.g., social engineering or phishing tests).	
	Intermediate	TA:G2.Q4	Management incorporates lessons learned from social engineering and phishing exercises to improve the employee awareness program lessons.	
		TA:G1.Q1 TA:G2.Q1	Cybersecurity awareness information is provided to retail customers and commercial clients at least annually.	Additional guidance—FFIEC requires that awareness information is provided to retail and commercial customers annually.
		TA:MIL5.Q1	Business units are provided cybersecurity training relevant to their particular business risks, over and above what is required of the institution as a whole.	
		TA:G2.Q3 TA:G2.Q4	The institution routinely updates its training to security staff to adapt to new threats.	
	Advanced	MIL2:Q4 – all	Independent directors are provided with cybersecurity training that addresses how complex products, services, and lines of business affect the institution's cyber risk.	Additional guidance—FFIEC requires that organizations should identify independent directors specifically and provide training on the need to address complex products, services, and lines of business as they relate to operational risk.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Innovative	TA MIL4.Q1	Key performance indicators are used to determine whether training and awareness programs positively influence behavior.	
CULTURE	Baseline	MIL3.Q1 – all	Management holds employees accountable for complying with the information security program. (FFIEC Information Security Booklet, page 7)	
	Evolving	TA:MIL2.Q2 TA:MIL2.Q4	The institution has formal standards of conduct that hold all employees accountable for complying with cybersecurity policies and procedures.	Additional guidance—FFIEC requires cybersecurity policies and procedures to be included in formal standards of conduct.
		RM:G4.Q1	Cyber risks are actively discussed at business unit meetings.	
		IM:G2.Q1	Employees have a clear understanding of how to identify and escalate potential cybersecurity issues.	Additional guidance—FFIEC requires that all employees are made aware of how to detect and report potential cybersecurity issues.
	Intermediate	IM:G1.Q3 MIL2.Q2 – all MIL2.Q3 – all	Management ensures performance plans are tied to compliance with cybersecurity policies and standards in order to hold employees accountable.	
		RM:G3.Q1 MIL5:Q1 – all	The risk culture requires formal consideration of cyber risks in all business decisions.	
		RM:G3.Q1	Cyber risk reporting is presented and discussed at the independent risk management meetings.	Additional guidance—FFIEC defines independent risk management meetings as internal to a line of business.
	Advanced	RM:MIL5.Q2	Management ensures continuous improvement of cyber risk cultural awareness.	
	Innovative	MIL5:Q2-all	The institution leads efforts to promote cybersecurity culture across the sector and to other sectors that they depend upon.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Domain 2: Threat Intelligence and Collaboration				
Assessment Factor: Threat Intelligence				
THREAT INTELLIGENCE AND INFORMATION	Baseline	VM:G2.Q1 VM:G2.Q2 SA:G1.Q1	The institution belongs or subscribes to a threat and vulnerability information sharing source(s) that provides information on threats (e.g., Financial Services Information Sharing and Analysis Center [FS-ISAC], U.S. Computer Emergency Readiness Team [US-CERT]). (FFIEC EBanking Work Program, page 28)	
		VM:G2.Q1 SA:G1.Q2	Threat information is used to monitor threats and vulnerabilities. (FFIEC Information Security Booklet, page 83)	
		VM:G2.Q1 RM:G5.Q1	Threat information is used to enhance internal risk management and controls. (FFIEC Information Security Booklet, page 4)	
	Evolving	SA:G1.Q2	Threat information received by the institution includes analysis of tactics, patterns, and risk mitigation recommendations.	Additional guidance—FFIEC requires that situational awareness procedures should include analysis of tactics, patterns, and risk mitigation recommendations.
	Intermediate	SA:G1.Q2 SA:G1.Q3	A formal threat intelligence program is implemented and includes subscription to threat feeds from external providers and internal sources.	
		SA:MIL2.Q3 SA:MIL2.Q4	Protocols are implemented for collecting information from industry peers and government.	
		Gap	A read-only, central repository of cyber threat intelligence is maintained.	
	Advanced	SA:MIL2.Q4	A cyber intelligence model is used for gathering threat information.	
		SA:G1.Q2	Threat intelligence is automatically received from multiple sources in real time.	Additional guidance—FFIEC requires that threat intelligence is automatically received from multiple sources in real time.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		SA:G1.Q2	The institution's threat intelligence includes information related to geopolitical events that could increase cybersecurity threat levels.	
	Innovative	Gap	A threat analysis system automatically correlates threat data to specific risks and then takes risk-based automated actions while alerting management.	
		Gap	The institution is investing in the development of new threat intelligence and collaboration mechanisms (e.g., technologies, business processes) that will transform how information is gathered and shared.	
MONITORING AND ANALYZING	Baseline	IM:G2.Q2	Audit log records and other security event logs are reviewed and retained in a secure manner. (FFIEC Information Security Booklet, page 79)	Additional guidance—FFIEC requires that event data logs include audit log records.
		IM:G2.Q8 IM:G2.Q9	Computer event logs are used for investigations once an event has occurred. (FFIEC Information Security Booklet, page 83)	
	Evolving	SA:G1.Q2	A process is implemented to monitor threat information to discover emerging threats.	
		VM:G2.Q5 SA:G1.Q3	The threat information and analysis process is assigned to a specific group or individual.	
		Gap	Security processes and technology are centralized and coordinated in a Security Operations Center (SOC) or equivalent.	
		VM:G2.Q3 VM:G2.Q5 IM:G3.Q3	Monitoring systems operate continuously with adequate support for efficient incident handling.	
	Intermediate	SA:G1.Q3	A threat intelligence team is in place that evaluates threat intelligence from multiple sources for credibility, relevance, and exposure.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		RM:G4.Q1	A profile is created for each threat that identifies the likely intent, capability, and target of the threat.	Additional guidance—FFIEC requires that risk analysis must include a threat profile.
		SA:G1.Q2	Threat information sources that address all components of the threat profile are prioritized and monitored.	
		RM:G4.Q1	Threat intelligence is analyzed to develop cyber threat summaries including risks to the institution and specific actions for the institution to consider.	
	Advanced	SA:G1.Q3	A dedicated cyber threat identification and analysis committee or team exists to centralize and coordinate initiatives and communications.	
		VM:G2.Q5	Formal processes have been defined to resolve potential conflicts in information received from sharing and analysis centers or other sources.	
		Gap	Emerging internal and external threat intelligence and correlated log analysis are used to predict future attacks.	
		RM.G2.Q2 RM:G5.Q1	Threat intelligence is viewed within the context of the institution's risk profile and risk appetite to prioritize mitigating actions in anticipation of threats.	
		CCM:G1.Q6	Threat intelligence is used to update architecture and configuration standards.	
	Innovative	Gap	The institution uses multiple sources of intelligence, correlated log analysis, alerts, internal traffic flows, and geopolitical events to predict potential future attacks and attack trends.	
		RM:G1.Q3	Highest risk scenarios are used to predict threats against specific business targets.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		VM:G2.Q3	IT systems automatically detect configuration weaknesses based on threat intelligence and alert management so actions can be prioritized.	Additional guidance—FFIEC requires that configuration weaknesses in IT systems are detected automatically.
Assessment Factor: Information Sharing				
INFORMATION SHARING	Baseline	SA:G2.Q1 SA:G3.Q1	Information security threats are gathered and shared with applicable internal employees. (FFIEC Information Security Booklet, page 83)	
		SA:G2.Q2	Contact information for law enforcement and the regulator(s) is maintained and updated regularly. (FFIEC Business Continuity Planning Work Program, Objective I: 5-1)	
		SA:G2.Q2	Information about threats is shared with law enforcement and regulators when required or prompted. (FFIEC Information Security Booklet, page 84)	
	Evolving	SA:G1.Q2 SA:G2.Q2	A formal and secure process is in place to share threat and vulnerability information with other entities.	
		SA:G1.Q1 SA:G3.Q1 VM:G2.Q1 VM:G2.Q2	A representative from the institution participates in law enforcement or information-sharing organization meetings.	
	Intermediate	SA:G2.Q1	A formal protocol is in place for sharing threat, vulnerability, and incident information to employees based on their specific job function.	
		SA:G3.Q1	Information-sharing agreements are used as needed or required to facilitate sharing threat information with other financial sector organizations or third parties.	Additional guidance—FFIEC requires that information sharing agreements are created as necessary.
		SA:G2.Q2 SA:G3.Q1	Information is shared proactively with the industry, law enforcement, regulators, and information-sharing forums.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		SA:G2.Q2	A process is in place to communicate and collaborate with the public sector regarding cyber threats.	
	Advanced	SA:G2.Q1	Management communicates threat intelligence with business risk context and specific risk management recommendations to the business units.	Additional guidance—FFIEC requires that risk context and risk management recommendations are included in communications with business units.
		SA:G1.Q2	Relationships exist with employees of peer institutions for sharing cyber threat intelligence.	
		RM:G4.Q1	A network of trust relationships (formal and/or informal) has been established to evaluate information about cyber threats.	
	Innovative	SA:G2.Q1	A mechanism is in place for sharing cyber threat intelligence with business units in real time including the potential financial and operational impact of inaction.	Additional guidance—FFIEC requires that threat information should include impact of inaction.
		RM:G4.Q1 RM:G4.Q2 RM:G5.Q1 RM G5.Q2	A system automatically informs management of the level of business risk specific to the institution and the progress of recommended steps taken to mitigate the risks.	Additional guidance—FFIEC requires that this must take place automatically.
		Gap	The institution is leading efforts to create new sector-wide information sharing channels to address gaps in external-facing information-sharing mechanisms.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Domain 3: Cybersecurity Controls				
Assessment Factor: Preventative Controls				
INFRASTRUCTURE MANAGEMENT	Baseline	CM:G2.Q2 CM:G2.Q8	Network perimeter defense tools (e.g., border router and firewall) are used. (FFIEC Information Security Booklet, page 33)	
		CM:G1.Q1	Systems that are accessed from the Internet or by external parties are protected by firewalls or other similar devices. (FFIEC Information Security Booklet, page 46)	Specific control objective
		CM:G1.Q1	All ports are monitored. (FFIEC Information Security Booklet, page 50)	Specific control objective
		CM:G1.Q1	Up to date antivirus and anti-malware tools are used. (FFIEC Information Security Booklet, page 78)	Specific control objective
		CCM:G3.Q1 CCM:G3.Q2 CCM:G3.Q3 CCM:G3.Q4	Systems configurations (for servers, desktops, routers, etc.) follow industry standards and are enforced. (FFIEC Information Security Booklet, page 56)	
		CM:G1.Q1	Ports, functions, protocols and services are prohibited if no longer needed for business purposes. (FFIEC Information Security Booklet, page 50)	Specific control objective
		AM:G5.Q1 CCM:G2.Q11	Access to make changes to systems configurations (including virtual machines and hypervisors) is controlled and monitored. (FFIEC Information Security Booklet, page 56)	
		CM:G1.Q1	Programs that can override system, object, network, virtual machine, and application controls are restricted. (FFIEC Information Security Booklet, page 41)	Specific control objective

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CM:G1.Q1	System sessions are locked after a pre-defined period of inactivity and are terminated after pre-defined conditions are met. (FFIEC Information Security Booklet, page 23)	Specific control objective
		CM:G1.Q1	Wireless network environments require security settings with strong encryption for authentication and transmission. (*N/A if there are no wireless networks.) (FFIEC Information Security Booklet, page 40)	Specific control objective
	Advanced	CM:G2.Q2	Network environments and virtual instances are designed and configured to restrict and monitor traffic between trusted and untrusted zones.	Additional guidance—FFIEC requires the monitoring of network traffic.
		CM:G1.Q1	Only one primary function is permitted per server to prevent functions that require different security levels from co-existing on the same server.	Specific control objective
		CM:G1.Q1	Anti-spoofing measures are in place to detect and block forged source IP addresses from entering the network.	Specific control objective
	Innovative	RM:G4.Q1 VM:G2.Q3 CCM:G1.Q2 CCM:G2.Q1 SA:G1.Q2	The institution risk scores all of its infrastructure assets and updates in real time based on threats, vulnerabilities, or operational changes.	Additional guidance for RM G4.Q1—FFIEC requires that aspects of other practices listed be updated and scored in real time.
		Gap	Automated controls are put in place based on risk scores to infrastructure assets, including automatically disconnecting affected assets.	
		CM:G3.Q1	The institution proactively seeks to identify control gaps that may be used as part of a zero-day attack.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CM:G1.Q1	Public-facing servers are routinely rotated and restored to a known clean state to limit the window of time a system is exposed to potential threats.	Specific control objective
ACCESS AND DATA MANAGEMENT	Baseline	AM:G5.Q5	Employee access is granted to systems and confidential data based on job responsibilities and the principles of least privilege. (FFIEC Information Security Booklet, page 19)	
		AM:G5.Q6	Employee access to systems and confidential data provides for separation of duties. (FFIEC Information Security Booklet, page 19)	
		AM:G5.Q3	Elevated privileges (e.g., administrator privileges) are limited and tightly controlled (e.g., assigned to individuals, not shared, and require stronger password controls). (FFIEC Information Security Booklet, page 19)	
		AM:G5.Q3	User access reviews are performed periodically for all systems and applications based on the risk to the application or system. (FFIEC Information Security Booklet, page 18)	
		AM:G5.Q2	Changes to physical and logical user access, including those that result from voluntary and involuntary terminations, are submitted to and approved by appropriate personnel. (FFIEC Information Security Booklet, page 18)	
		AM:G5.Q2 AM:G5.Q3	Identification and authentication are required and managed for access to systems, applications, and hardware. (FFIEC Information Security Booklet, page 21)	
		AM:G5.Q1	Access controls include password complexity and limits to password attempts and reuse. (FFIEC Information Security Booklet, page 66)	Additional guidance—FFIEC requires that access controls for information and technology assets include password complexity and attempt limits.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		AM:G5.Q3 AM:G5.Q4	All default passwords and unnecessary default accounts are changed before system implementation. (FFIEC Information Security Booklet, page 61)	Additional guidance—FFIEC requires a review of default passwords and accounts.
		Gap	Customer access to Internet-based products or services requires authentication controls (e.g., layered controls, multifactor) that are commensurate with the risk. (FFIEC Information Security Booklet, page 21)	
		CCM:G2.Q7	Production and non-production environments are segregated to prevent unauthorized access or changes to information assets. (*N/A if no production environment exists at the institution or the institution's third party.) (FFIEC Information Security Booklet, page 64)	
		AM:G5.Q1	Physical security controls are used to prevent unauthorized access to information systems and telecommunication systems. (FFIEC Information Security Booklet, page 47)	
		CM:G2.Q3 CM:G2.Q4	All passwords are encrypted in storage and in transit. (FFIEC Information Security Booklet, page 21)	
		CM:G2.Q4	Confidential data is encrypted when transmitted across public or untrusted networks (e.g., Internet). (FFIEC Information Security Booklet, page 51)	
		CM:G2.Q3	Mobile devices (e.g., laptops, tablets, and removable media) are encrypted if used to store confidential data. (*N/A if mobile devices are not used.) (FFIEC Information Security Booklet, page 51)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		AM:G5-Q1	Remote access to critical systems by employees, contractors, and third parties uses encrypted connections and multifactor authentication. (FFIEC Information Security Booklet, page 45)	Additional guidance—FFIEC requires that access granted to remote individuals must use encrypted connections.
		CCM:G1.Q1	Administrative, physical, or technical controls are in place to prevent users without administrative responsibilities from installing unauthorized software. (FFIEC Information Security Booklet, page 25)	
		Gap	Customer service (e.g., the call center) utilizes formal procedures to authenticate customers commensurate with the risk of the transaction or request. (FFIEC Information Security Booklet, page 19)	
		AM:G6.Q6 AM:G6.Q7	Data is disposed of or destroyed according to documented requirements and within expected time frames. (FFIEC Information Security Booklet, page 66)	
	Evolving	AM:G5.Q3	Changes to user access permissions trigger automated notices to appropriate personnel.	Additional guidance—FFIEC requires that automated notifications are generated when user access permissions change.
		Gap	Administrators have two accounts: one for administrative use and one for general purpose, non-administrative tasks.	
		Gap	Use of customer data in non-production environments complies with legal, regulatory, and internal policy requirements for concealing or removing of sensitive data elements.	
		AM:G5.Q1	Physical access to high-risk or confidential systems is restricted and logged, and unauthorized access is blocked.	
		CM:G2Q5	Controls are in place to prevent unauthorized access to cryptographic keys.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Intermediate	CM:G2.Q5	The institution has implemented tools to prevent unauthorized access to or exfiltration of confidential data.	
		CM:G2.Q5	Controls are in place to prevent unauthorized escalation of user privileges.	
		CM:G2.Q1	Access controls are in place for database administrators to prevent unauthorized downloading or transmission of confidential data.	Specific control objective
		Gap	All physical and logical access is removed immediately upon notification of involuntary termination and within 24 hours of an employee's voluntary departure.	
		Gap	Multifactor authentication and/or layered controls have been implemented to secure all third-party access to the institution's network and/or systems and applications.	Possibly related to EDM:G3.Q4 and CM:G2.Q1
		Gap	Multifactor authentication (e.g., tokens, digital certificates) techniques are used for employee access to high-risk systems as identified in the risk assessment(s). (*N/A if no high risk systems.)	Possibly related to CM:G2.Q1
		CM:G2.Q4	Confidential data are encrypted in transit across private connections (e.g., frame relay and T1) and within the institution's trusted zones.	
		Gap	Controls are in place to prevent unauthorized access to collaborative computing devices and applications (e.g., networked white boards, cameras, microphones, online applications such as instant messaging and document sharing). (* N/A if collaborative computing devices are not used.)	Possibly related to CM:G2.Q1

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Advanced	AM:G6.Q1	Encryption of select data at rest is determined by the institution's data classification and risk assessment.	
		Gap	Customer authentication for high-risk transactions includes methods to prevent malware and man-in-the-middle attacks (e.g., using visual transaction signing).	Possibly related to CM:G2.Q1
	Innovative	Gap	Adaptive access controls de-provision or isolate an employee, third-party, or customer credentials to minimize potential damage if malicious behavior is suspected.	
		Gap	Unstructured confidential data are tracked and secured through an identity-aware, cross-platform storage system that protects against internal threats, monitors user access, and tracks changes.	
		Gap	Tokenization is used to substitute unique values for confidential information (e.g., virtual credit card).	
		Gap	The institution is leading efforts to create new technologies and processes for managing customer, employee, and third-party authentication and access.	
		Gap	Real-time risk mitigation is taken based on automated risk scoring of user credentials.	
DEVICE/END-POINT SECURITY	Baseline	CM:G2.Q7	Controls are in place to restrict the use of removable media to authorized personnel. (FFIEC Information Security Work Program, Objective I: 4-1)	
	Evolving	Gap	Tools automatically block attempted access from unpatched employee and third-party devices.	Possibly related to CM:G2.Q1
		Gap	Tools automatically block attempted access by unregistered devices to internal networks.	Possibly related to CM:G2.Q1

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		Gap	The institution has controls to prevent the unauthorized addition of new connections.	Possibly related to CM:G2.Q1
		CM:G2.Q7	Controls are in place to prevent unauthorized individuals from copying confidential data to removable media.	
		VM:G1.Q3 VM:G1.Q4 VM:G1.Q5 IM:G2.Q1	Antivirus and anti-malware tools are deployed on end-point devices (e.g., workstations, laptops, and mobile devices).	
		Gap	Mobile devices with access to the institution's data are centrally managed for antivirus and patch deployment. (*N/A if mobile devices are not used.)	Possibly related to CM:G2.Q1
		CM:G2.Q5	The institution wipes data remotely on mobile devices when a device is missing or stolen. (*N/A if mobile devices are not used.)	Additional guidance—FFIEC requires that controls include the ability to remotely wipe data from wireless devices.
	Intermediate	CM:G2.Q5	Data loss prevention controls or devices are implemented for inbound and outbound communications (e.g., email, FTP, Telnet, prevention of large file transfers).	
		CCM:G2.Q2	Mobile device management includes integrity scanning (e.g., jailbreak/rooted detection). (*N/A if mobile devices are not used.)	
		Gap	Mobile devices connecting to the corporate network for storing and accessing company information allow for remote software version/patch validation. (*N/A if mobile devices are not used.)	Possibly related to CM:G2.Q1
	Advanced	Gap	Employees' and third parties' devices (including mobile) without the latest security patches are quarantined and patched before the device is granted access to the network.	Possibly related to CM:G2.Q1

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		Gap	Confidential data and applications on mobile devices are only accessible via a secure, isolated sandbox or a secure container.	Possibly related to CM:G2.Q1
	Innovative	Gap	A centralized end-point management tool provides fully integrated patch, configuration, and vulnerability management, while also being able to detect malware upon arrival to prevent an exploit.	Possibly related to CM:G2.Q1
SECURE CODING	Baseline	CCM:G1.Q6	Developers working for the institution follow secure program coding practices, as part of a system development life cycle (SDLC), that meet industry standards. (FFIEC Information Security Booklet, page 56)	
		CCM:G2.Q7	The security controls of internally developed software are periodically reviewed and tested. (*N/A if there is no software development.) (FFIEC Information Security Booklet, page 59)	Additional guidance—FFIEC requires that, for internally developed software, security controls must be periodically reviewed.
		CCM:G2.Q7	The security controls in internally developed software code are independently reviewed before migrating the code to production. (*N/A if there is no software development.) (FFIEC Development and Acquisition Booklet, page 2)	Additional guidance—FFIEC requires that the security controls in internally developed software be independently reviewed.
		Gap	Intellectual property and production code are held in escrow. (*N/A if there is no production code to hold in escrow.) (FFIEC Development and Acquisition Booklet, page 39)	Possibly related to CCM:G3.Q1
	Evolving	CCM:G1.Q6	Security testing occurs at all post-design phases of the SDLC for all applications, including mobile applications. (*N/A if there is no software development.)	
	Intermediate	VM:G3.Q1	Processes are in place to mitigate vulnerabilities identified as part of the secure development of systems and applications.	Additional guidance—FFIEC requires that the organization should examine internal development practices when identifying vulnerabilities.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CCM:G2.Q7	The security of applications, including Web-based applications connected to the Internet, is tested against known types of cyber attacks (e.g., SQL injection, cross-site scripting, buffer overflow) before implementation or following significant changes.	
		CCM:G2.Q2	Software code executables and scripts are digitally signed to confirm the software author and guarantee that the code has not been altered or corrupted.	
		RM:G4.Q1	A risk-based, independent information assurance function evaluates the security of internal applications.	Additional guidance—FFIEC requires that the security of internal applications is an explicit risk category.
	Advanced	VM:G3.Q1	Vulnerabilities identified through a static code analysis are remediated before implementing newly developed or changed applications into production.	
		AM:G3.Q1	All interdependencies between applications and services have been identified.	
		CCM:G2.Q7	Independent code reviews are completed on internally developed or vendor-provided custom applications to ensure there are no security gaps.	
	Innovative	Gap	Software code is actively scanned by automated tools in the development environment so that security weaknesses can be resolved immediately during the design phase.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Assessment Factor: Detective Controls				
THREAT AND VULNERABILITY DETECTION	Baseline	VM:G2.Q3	Independent testing (including penetration testing and vulnerability scanning) is conducted according to the risk assessment for external facing systems and the internal network. (FFIEC Information Security Booklet, page 61)	
		VM:G1.Q3 VM:G1.Q4 VM:G1.Q5 IM:G2.Q1	Antivirus and anti-malware tools are used to detect attacks. (FFIEC Information Security Booklet, page 55)	
		VM:G1.Q2	Firewall rules are audited or verified at least quarterly. (FFIEC Information Security Booklet, page 82)	Additional guidance—FFIEC requires that firewall rules are part of the standard set of tools and must be audited at least quarterly.
		VM:G1.Q3	Email protection mechanisms are used to filter for common cyber threats (e.g., attached malware or malicious links). (FFIEC Information Security Booklet, page 39)	
	Evolving	VM:G2.Q3	Independent penetration testing of network boundary and critical web-facing applications is performed routinely to identify security control gaps.	
		CCM:G2.Q7 VM:G2.Q3	Independent penetration testing is performed on Internet-facing applications or systems before they are launched or undergo significant change.	
		VM:G2.Q2	Antivirus and anti-malware tools are updated automatically.	
		VM:G2.Q2 VM:G3.Q1	Firewall rules are updated routinely.	
		VM:G2.Q3 CCM:G2.Q7	Vulnerability scanning is conducted and analyzed before deployment/redeployment of new/existing devices.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CCM:G2.Q5	Processes are in place to monitor potential insider activity that could lead to data theft or destruction.	
	Intermediate	EDM:G4.Q1 EDM:G4.Q2	Audit or risk management resources review the penetration testing scope and results to help determine the need for rotating companies based on the quality of the work.	
		VM:G1.Q3	Emails and attachments are automatically scanned to detect malware and are blocked when malware is present.	Additional guidance—FFIEC requires that email be automatically scanned and blocked if it contains malware.
	Advanced	VM:G2.Q3	Weekly vulnerability scanning is rotated among environments to scan all environments throughout the year.	
		Gap	Penetration tests include cyber attack simulations and/or real-world tactics and techniques such as red team testing to detect control gaps in employee behavior, security defenses, policies, and resources.	Possibly related to VM:G2.Q3
		Gap	Automated tool(s) proactively identifies high-risk behavior signaling an employee who may pose an insider threat.	
	Innovative	Gap	User tasks and content (e.g., opening an email attachment) are automatically isolated in a secure container or virtual environment so that malware can be analyzed but cannot access vital data, end-point operating systems, or applications on the institution's network.	
		VM:G2.Q3	Vulnerability scanning is performed on a weekly basis across all environments.	Additional guidance—FFIEC requires that vulnerability scanning be performed weekly.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
ANOMALOUS ACTIVITY DETECTION	Baseline	CCM:G1.Q2	The institution is able to detect anomalous activities through monitoring across the environment. (FFIEC Information Security Booklet, page 32)	
		IM:G2.Q1	Customer transactions generating anomalous activity alerts are monitored and reviewed. (FFIEC Wholesale Payments Booklet, page 12)	
		IM:G5.Q1	Logs of physical and/or logical access are reviewed following events. (FFIEC Information Security Booklet, page 73)	
		IM:G2.Q1	Access to critical systems by third parties is monitored for unauthorized or unusual activity. (FFIEC Outsourcing Booklet, page 26)	
		AM:G5.Q3	Elevated privileges are monitored. (FFIEC Information Security Booklet, page 19)	
	Evolving	IM:G2.Q1	Systems are in place to detect anomalous behavior automatically during customer, employee, and third-party authentication.	
		IM:G2.Q1	Security logs are reviewed regularly.	
		Gap	Logs provide traceability for all system access by individual users.	
		IM:G3.Q2	Thresholds have been established to determine activity within logs that would warrant management response.	
	Intermediate	CM:G2.Q1 IM:G2.Q1	Online customer transactions are actively monitored for anomalous behavior.	
		CM:G2.Q1 IM:G2.Q1	Tools to detect unauthorized data mining are used.	
		IM:G3.Q2	Tools actively monitor security logs for anomalous behavior and alert within established parameters.	Additional guidance—FFIEC requires that alert criteria for tools monitoring security logs is established.
		IM:G2.Q2	Audit logs are backed up to a centralized log server or media that is difficult to alter.	Additional guidance—FFIEC requires that the logs should be centrally maintained and difficult to alter.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		IM:G3.Q2	Thresholds for security logging are evaluated periodically.	Additional guidance—FFIEC requires thresholds be evaluated periodically.
		IM:G2.Q4	Anomalous activity and other network and system alerts are correlated across business units to detect and prevent multifaceted attacks (e.g., simultaneous account takeover and DDoS attack).	
	Advanced	Gap	An automated tool triggers system and/or fraud alerts when customer logins occur within a short period of time but from physically distant IP locations.	Possibly related to CM:G2.Q1
		Gap	External transfers from customer accounts generate alerts and require review and authorization if anomalous behavior is detected.	Possibly related to CM:G2.Q1
		IM:G2.Q1	A system is in place to monitor and analyze employee behavior (network use patterns, work hours, and known devices) to alert on anomalous activities.	
		Gap	An automated tool(s) is in place to detect and prevent data mining by insider threats.	Possibly related to CM:G2.Q1
		Gap	Tags on fictitious confidential data or files are used to provide advanced alerts of potential malicious activity when the data is accessed.	
	Innovative	Gap	The institution has a mechanism for real-time automated risk scoring of threats.	
		Gap	The institution is developing new technologies that will detect potential insider threats and block activity in real time.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
EVENT DETECTION	Baseline	CCM:G3.Q3 CCM:G3.Q5	A normal network activity baseline is established. (FFIEC Information Security Booklet, page 77)	
		IM:G2.Q1	Mechanisms (e.g., antivirus alerts, log event alerts) are in place to alert management to potential attacks. (FFIEC Information Security Booklet, page 78)	
		VM:G1.Q5	Processes are in place to monitor for the presence of unauthorized users, devices, connections, and software. (FFIEC Information Security Work Program, Objective II: M-9)	
		IM:G1.Q1 IM:G1.Q3 IM:G1.Q4 IM:G2.Q1 CCM:G2.Q6	Responsibilities for monitoring and reporting suspicious systems activity have been assigned. (FFIEC Information Security Booklet, page 83)	
		IM:G2.Q1	The physical environment is monitored to detect potential unauthorized access. (FFIEC Information Security Booklet, page 47)	
	Evolving	IM:G2.Q4	A process is in place to correlate event information from multiple sources (e.g., network, application, or firewall).	
	Intermediate	CM:G2.Q5	Controls or tools (e.g., data loss prevention) are in place to detect potential unauthorized or unintentional transmissions of confidential data.	
		IM:MIL4.Q1	Event detection processes are proven reliable.	
		CM:G2.Q1 IM:G2.Q1	Specialized security monitoring is used for critical assets throughout the infrastructure.	
	Advanced	CCM:G2.Q5	Automated tools detect unauthorized changes to critical system files, firewalls, intrusion prevention systems, intrusion detection systems, or other security devices.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CCM:G2.Q2 SA:G1.Q2	Real-time network monitoring and detection is implemented and incorporates sector-wide event information.	
		CCM:G2.Q2 CCM:G2.Q6	Real-time alerts are automatically sent when unauthorized software, hardware, or asset changes occur.	Additional guidance—FFIEC requires real-time notification of changes to assets.
		IM:G2.Q4	Tools are in place to actively correlate event information from multiple sources and send alerts based on established parameters.	
	Innovative	Gap	The institution is leading efforts to develop event detection systems that will correlate in real time when events are about to occur.	
		Gap	The institution is leading the development effort to design new technologies that will detect potential insider threats and block activity in real time.	
Assessment Factor: Corrective Controls				
PATCH MANAGEMENT	Baseline	CCM:G1.Q1	A patch management program is implemented and ensures that software and firmware patches are applied in a timely manner. (FFIEC Information Security Booklet, page 62)	
		CCM:G2.Q7	Patches are tested before being applied to systems and/or software. (FFIEC Operations Booklet, page 22)	
		CCM:MIL3.Q1	Patch management reports are reviewed and reflect missing security patches. (FFIEC Development and Acquisition Booklet, page 50)	
	Evolving	CCM:G1.Q1	A formal process is in place to acquire, test, and deploy software patches based on criticality.	
		Gap	Systems are configured to retrieve patches automatically.	
		CCM:G2.Q7	Operational impact is evaluated before deploying security patches.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		Gap	An automated tool(s) is used to identify missing security patches as well as the number of days since each patch became available.	
		VM:G3.Q3	Missing patches across all environments are prioritized and tracked.	
	Intermediate	CCM:G2.Q1 RM:G5.Q2	Patches for high-risk vulnerabilities are tested and applied when released or the risk is accepted and accountability assigned.	
	Advanced	Gap	Patch monitoring software is installed on all servers to identify any missing patches for the operating system software, middleware, database, and other key software.	
		CCM:G2.Q1	The institution monitors patch management reports to ensure security patches are tested and implemented within aggressive time frames (e.g., 0-30 days).	Additional guidance—FFIEC requires that patches be implemented within aggressive time frames.
	Innovative	Gap	The institution develops security patches or bug fixes or contributes to open source code development for systems it uses.	
		CCM:G2.Q7	Segregated or separate systems are in place that mirror production systems allowing for rapid testing and implementation of patches and provide for rapid fallback when needed.	Additional guidance—FFIEC requires a separate test environment which can also serve as a fallback system when needed.
REMEDIATION	Baseline	Gap	Issues identified in assessments are prioritized and resolved based on criticality and within the time frames established in the response to the assessment report. (FFIEC Information Security Booklet, page 87)	Possibly related to VM:G2.Q4, not clear which “assessment report” is referenced
	Evolving	AM:G6.Q6	Data is destroyed or wiped on hardware and portable/mobile media when a device is missing, stolen, or no longer needed.	
		VM:G3.Q1	Formal processes are in place to resolve weaknesses identified during penetration testing.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Intermediate	Gap	Remediation efforts are confirmed by conducting a follow-up vulnerability scan.	
		Gap	Penetration testing is repeated to confirm that medium- and high-risk, exploitable vulnerabilities have been resolved.	
		IM:G2.Q8 IM:G2.Q9 IM:G5.Q1	Security investigations, forensic analysis, and remediation are performed by qualified staff or third parties.	
		IM:G2.Q8 IM:G2.Q9 IM:G5.Q1	Generally accepted and appropriate forensic procedures, including chain of custody, are used to gather and present evidence to support potential legal action.	
		AM:G5.Q1 CCM:G2.Q10	The maintenance and repair of organizational assets are performed by authorized individuals with approved and controlled tools.	
		CCM:G2.Q9	The maintenance and repair of organizational assets are logged in a timely manner.	
	Advanced	Gap	All medium and high risk issues identified in penetration testing, vulnerability scanning, and other independent testing are escalated to the board or an appropriate board committee for risk acceptance if not resolved in a timely manner.	Possibly related to RM:G4.Q2 but seems to define a policy requirement
	Innovative	Gap	The institution is developing technologies that will remediate systems damaged by zero-day attacks to maintain current recovery time objectives.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Domain 4: External Dependency Management				
Assessment Factor: Connections				
CONNECTIONS	Baseline	EDM:G1.Q1 EDM:G1.Q2 EDM:G1.Q3 EDM:G3.Q3 EDM:G5.Q1 EDM:G5.Q2	The critical business processes that are dependent on external connectivity have been identified. (FFIEC Information Security Booklet, page 9)	
		EDM:G3.Q1	The institution ensures that third-party connections are authorized. (FFIEC Information Security Booklet, page 17)	
		AM:G2.Q1	A network diagram is in place and identifies all external connections. (FFIEC Information Security Booklet, page 9)	
		AM:G2.Q5 CCM:G3.Q5 CCM:G3.Q6	Data flow diagrams are in place and document information flow to external parties. (FFIEC Information Security Booklet, page 10)	
	Evolving	EDM:G1Q1	Critical business processes have been mapped to the supporting external connections.	
		EDM:G1.Q2	The network diagram is updated when connections with third parties change or at least annually.	Additional guidance—FFIEC specifies the use of a network diagram to track connections.
		SCM:G1.Q1 SCM:G1.Q2 SCM:G1.Q5	Network and systems diagrams are stored in a secure manner with proper restrictions on access.	
		CCM:G2.Q5 EDM:G4.Q1 EDM:G4.Q2	Controls for primary and backup third-party connections are monitored and tested on a regular basis.	
	Intermediate	AM:G2.Q5	A validated asset inventory is used to create comprehensive diagrams depicting data repositories, data flow, infrastructure, and connectivity.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		EDM:G4.Q1	Security controls are designed and verified to detect and prevent intrusions from third-party connections.	
		CCM:G2.Q5 EDM:G4.Q1	Monitoring controls cover all external connections (e.g., third-party service providers, business partners, customers).	
		CCM:G2.Q5	Monitoring controls cover all internal network-to-network connections.	
	Advanced	CCM:G1.Q1	The security architecture is validated and documented before network connection infrastructure changes.	
		EDM:G4.Q1	The institution works closely with third-party service providers to maintain and improve the security of external connections.	
	Innovative	Gap	Diagram(s) of external connections is interactive, shows real-time changes to the network connection infrastructure, new connections, and volume fluctuations, and alerts when risks arise.	
		CM:G2.Q1	The institution's connections can be segmented or severed instantaneously to prevent contagion from cyber attacks.	Additional guidance—FFIEC requires that connections may be segmented or severed instantaneously.
Assessment Factor: Relationship Management				
DUE DILIGENCE	Baseline	EDM:G3.Q3	Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls. (FFIEC Information Security Booklet, page 69)	
		EDM:G1.Q2	A list of third-party service providers is maintained. (FFIEC Outsourcing Booklet, page 19)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		EDM:G2.Q1	A risk assessment is conducted to identify criticality of service providers. (FFIEC Outsourcing Booklet, page 6)	
	Evolving	EDM:G4.Q1	A formal process exists to analyze assessments of third-party cybersecurity controls.	
		EDM:MIL4.Q1	The board or an appropriate board committee reviews a summary of due diligence results including management's recommendations to use third parties that will affect the institution's inherent risk profile.	
	Intermediate	EDM:G2.Q1	A process is in place to confirm that the institution's third-party service providers conduct due diligence of their third parties (e.g., subcontractors).	
		EDM:G3.Q3	Pre-contract, physical site visits of high-risk vendors are conducted by the institution or by a qualified third party.	Additional guidance—FFIEC requires physical site visits to high-risk vendors.
	Advanced	EDM:MIL2.Q1	A continuous process improvement program is in place for third-party due diligence activity.	
		EDM:G4.Q1	Audits of high-risk vendors are conducted on an annual basis.	Additional guidance—FFIEC requires annual audits of high risk vendors.
	Innovative	Gap	The institution promotes sector-wide efforts to build due diligence mechanisms that lead to in-depth and efficient security and resilience reviews.	
		Gap	The institution is leading efforts to develop new auditable processes and for conducting due diligence and ongoing monitoring of cybersecurity risks posed by third parties.	
CONTRACTS	Baseline	EDM:G3.Q4	Formal contracts that address relevant security and privacy requirements are in place for all third parties that process, store, or transmit confidential data or provide critical services. (FFIEC Information Security Booklet, page 7)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		EDM:G3.Q4	Contracts acknowledge that the third party is responsible for the security of the institution's confidential data that it possesses, stores, processes, or transmits. (FFIEC Information Security Booklet, page 12)	
		EDM:G4.Q1	Contracts stipulate that the third-party security controls are regularly reviewed and validated by an independent party. (FFIEC Information Security Booklet, page 12)	Additional guidance—FFIEC requires that an independent party conduct monitoring.
		EDM:G4.Q3	Contracts identify the recourse available to the institution should the third party fail to meet defined security requirements. (FFIEC Outsourcing Booklet, page 12)	
		EDM:G3.Q4	Contracts establish responsibilities for responding to security incidents. (FFIEC E-Banking Booklet, page 22)	Additional guidance—FFIEC requires that contracts must establish responsibility for responding to incidents.
		EDM:G3.Q4	Contracts specify the security requirements for the return or destruction of data upon contract termination. (FFIEC Outsourcing Booklet, page 15)	
	Evolving	EDM:G3.Q4	Responsibilities for managing devices (e.g., firewalls, routers) that secure connections with third parties are formally documented in the contract.	
		EDM:G3.Q4	Responsibility for notification of direct and indirect security incidents and vulnerabilities is documented in contracts or service-level agreements (SLAs).	
		EDM:G3.Q4	Contracts stipulate geographic limits on where data can be stored or transmitted.	
	Intermediate	EDM:G3.Q4	Third-party SLAs or similar means are in place that require timely notification of security events.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Advanced	EDM:G3.Q3	Contracts require third-party service provider's security policies meet or exceed those of the institution.	
		EDM:G3.Q1	A third-party termination/exit strategy has been established and validated with management.	
	Innovative	Gap	The institution promotes a sector-wide effort to influence contractual requirements for critical third parties to the industry.	
ONGOING MONITORING	Baseline	RM:MIL4.Q1 EDM:G2.Q1	The third-party risk assessment is updated regularly. (FFIEC Outsourcing Booklet, page 3)	
		EDM:G4.Q1	Audits, assessments, and operational performance reports are obtained and reviewed regularly, validating security controls for critical third parties. (FFIEC Information Security Booklet, page 86)	
		EDM:G4.Q1	Ongoing monitoring practices include reviewing critical third parties' resilience plans. (FFIEC Outsourcing Booklet, page 19)	Additional guidance—FFIEC requires a review of third party resilience plans.
	Evolving	EDM:G1.Q2	A process to identify new third-party relationships is in place, including identifying new relationships that were established without formal approval.	
		EDM:G4.Q1	A formal program assigns responsibility for ongoing oversight of third party access.	
		EDM:G1.Q3	Monitoring of third parties is scaled, in terms of depth and frequency, according to the risk of the third parties.	
		Gap	Automated reminders or ticklers are in place to identify when required third-party information needs to be obtained or analyzed	
	Intermediate	AM:G5.Q5	Third-party employee access to the institution's confidential data is tracked actively based on the principles of least privilege.	Additional guidance—FFIEC requires that third-party employee access to an organization's confidential data is tracked.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		EDM:G4.Q1	Periodic on-site assessments of high-risk vendors are conducted to ensure appropriate security controls are in place.	Additional guidance—FFIEC requires physical site visits to high-risk vendors.
	Advanced	Gap	Third-party employee access to confidential data on third-party hosted systems is tracked actively via automated reports and alerts.	
	Innovative	Gap	The institution is leading efforts to develop new auditable processes for ongoing monitoring of cybersecurity risks posed by third parties.	
Domain 5: Cyber Incident Management and Resilience				
Assessment Factor: Incident Resilience Planning and Strategy				
PLANNING	Baseline	IM:G4.Q2	The institution has documented how it will react and respond to cyber incidents. (FFIEC Business Continuity Planning Booklet, page 4)	
		IM:G2.Q1	Communication channels exist to provide employees a means for reporting information security events in a timely manner. (FFIEC Information Security Booklet, page 83)	
		IM:G1.Q4 SCM:G1.Q3	Roles and responsibilities for incident response team members are defined. (FFIEC Information Security Booklet, page 84)	
		IM:G1.Q4	The response team includes individuals with a wide range of backgrounds and expertise, from many different areas within the institution (e.g., management, legal, public relations, as well as information technology). (FFIEC Information Security Booklet, page 84)	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		AM:G2.Q2 AM:G3.Q2 AM:G6.Q5 AM:G7.Q3 SCM:G1Q1 SCM:G1.Q6 SCM:G3.Q4 EDM:G3.Q1 EDM:G3.Q2 EDM:G3.Q4	A formal backup and recovery plan exists for all critical business lines. (FFIEC Business Continuity Planning Booklet, page 4)	
		SCM:G1.Q1 SCM.G4.Q1	The institution plans to use business continuity, disaster recovery, and data backup programs to recover operations following an incident. (FFIEC Information Security Booklet, page 71)	
	Evolving	IM:G4.Q2 SCM:G1.Q6	The remediation plan and process outlines the mitigating actions, resources, and time parameters.	
		SCM:G1.Q1	The corporate disaster recovery, business continuity, and crisis management plans have integrated consideration of cyber incidents.	Additional guidance—FFIEC requires that disaster recovery, business continuity, and crisis management be included in Service Continuity planning.
		AM:G2.Q2 AM:G3.Q2 AM:G6.Q5 AM:G7.Q3 SCM:G1Q1 SCM:G1.Q6 SCM:G3.Q4 EDM:G3.Q1 EDM:G3.Q2 EDM:G3.Q4	Alternative processes have been established to continue critical activity within a reasonable time period.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		AM:G1.Q2	Business impact analyses have been updated to include cybersecurity.	Additional guidance—FFIEC requires that cybersecurity events be considered when conducting a business impact analysis.
		IM:G1.Q4 EDM:G1.Q2	Due diligence has been performed on technical sources, consultants, or forensic service firms that could be called to assist the institution during or following an incident.	
	Intermediate	IM:G4.Q1 IM:G4.Q2 IM:G4.Q3 SCM:G1.Q4	A strategy is in place to coordinate and communicate with internal and external stakeholders during or following a cyber attack.	
		IM:G4.Q2	Plans are in place to re-route or substitute critical functions and/or services that may be affected by a successful attack on Internet-facing systems.	
		IM:G4.Q2	A direct cooperative or contractual agreement(s) is in place with an incident response organization(s) or provider(s) to assist rapidly with mitigation efforts.	
		VM:G4.Q1 IM:G5.Q1 IM:G5.Q2 IM:G5.Q3 SCM:G4.Q3	Lessons learned from real-life cyber incidents and attacks on the institution and other organizations are used to improve the institution's risk mitigation capabilities and response plan.	
	Advanced	SCM:G1.Q1	Methods for responding to and recovering from cyber incidents are tightly woven throughout the business units' disaster recovery, business continuity, and crisis management plans.	
		MIL2.Q1 – all	Multiple systems, programs, or processes are implemented into a comprehensive cyber resilience program to sustain, minimize, and recover operations from an array of potentially disruptive and destructive cyber incidents.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		MIL5.Q2 – all	A process is in place to continuously improve = resilience	
	Innovative	IM:MIL2.Q1	The incident response plan is designed to ensure recovery from disruption of services, assurance of data integrity, and recovery of lost or corrupted data following a cybersecurity incident.	
		IM:G4.Q2	The incident response process includes detailed actions and rule-based triggers for automated response.	
TESTING	Baseline	IM:G4.Q2 SCM:G3.Q1 SCM:G3.Q3	Scenarios are used to improve incident detection and response. (FFIEC Information Security Booklet, page 71)	
		SCM:G3.Q1	Business continuity testing involves collaboration with critical third parties. (FFIEC Business Continuity Planning Booklet, page J-6)	Additional guidance—FFIEC requires that testing includes critical third parties.
		SCM:G3.Q2	Systems, applications, and data recovery is tested at least annually. (FFIEC Business Continuity Planning Booklet, page J-7)	Additional guidance—FFIEC requires that data recovery is tested “at least annually.”
	Evolving	IM:G4.Q2 SCM:G1.Q1 SCM:G1.Q6 SCM:G3.Q4	Recovery scenarios include plans to recover from data destruction and impacts to data integrity, data loss, and system and data availability.	
		SCM:G3.Q5	Widely reported events are used to evaluate and improve the institution's response.	
		SCM:G3.Q4	Information backups are tested periodically to verify they are accessible and readable.	
	Intermediate	RM:G4.Q1	Cyber-attack scenarios are analyzed to determine potential impact to critical business processes.	Additional guidance—FFIEC requires cyber-attack scenarios be included in risk analysis.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		Gap	The institution participates in sector-specific cyber exercises or scenarios (e.g., FS-ISAC Cyber Attack (against) Payment Processors [CAPP]).	
		SCM:G3.Q1	Resilience testing is based on analysis and identification of realistic and highly likely threats as well as new and emerging threats facing the institution.	
		SCM:G3.Q1	The critical online systems and processes are tested to withstand stresses for extended periods (e.g., DDoS).	
		IM:G5.Q3 SCM:G3.Q5 SCM:G4.Q3	The results of cyber event exercises are used to improve the incident response plan and automated triggers.	
	Advanced	SCM:G3.Q3 SCM:MIL2.Q1	Resilience testing is comprehensive and coordinated across all critical business functions.	
		SCM:G3.Q1	The institution validates that it is able to recover from cyber events similar to known sophisticated attacks at other organizations.	
		SCM:G3.Q1 SCM:G3.Q3	Incident response testing evaluates the institution from an attacker's perspective to determine how the institution or its assets at critical third parties may be targeted.	
		SCM:G3.Q5	The institution corrects root causes for problems discovered during cybersecurity resilience testing.	
		SCM:G3.Q1 SCM:G3.Q3	Cybersecurity incident scenarios involving significant financial loss are used to stress test the institution's risk management.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
	Innovative	Gap	The institution tests the ability to shift business processes or functions between different processing centers or technology systems for cyber incidents without interruption to business or loss of productivity or data.	
		SCM:G3.Q3	The institution has validated that it is able to remediate systems damaged by zero-day attacks to maintain current recovery time objectives.	
		Gap	The institution is leading the development of more realistic test environments.	
		Gap	Cyber incident scenarios are used to stress test potential financial losses across the sector.	
Assessment Factor: Detection, Response, and Mitigation				
DETECTION	Baseline	IM:G3.Q2	Alert parameters are set for detecting information security incidents that prompt mitigating actions. (FFIEC Information Security Booklet, page 43)	
		CM:G1.Q1	System performance reports contain information that can be used as a risk indicator to detect information security incidents. (FFIEC Information Security Booklet, page 86)	
		IM:G2.Q1 IM:G3.Q2	Tools and processes are in place to detect, alert, and trigger the incident response program. (FFIEC Information Security Booklet, page 84)	
	Evolving	IM:G2.Q1	The institution has processes to detect and alert the incident response team when potential insider activity manifests that could lead to data theft or destruction.	
	Intermediate	IM:G3.Q2	The incident response program is triggered when anomalous behaviors and attack patterns or signatures are detected.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CM:G1.Q1 IM:G2.Q1	The institution has the ability to discover infiltration before the attacker traverses across systems, establishes a foothold, steals information, or causes damage to data and systems.	
		IM:G2.Q1 IM:G3.Q1 IM:G3.Q2 IM:G4.Q1	Incidents are detected in real time through automated processes that include instant alerts to appropriate personnel who can respond.	
		IM:G2.Q4	Network and system alerts are coordinated across business units to better detect and prevent multifaceted attacks (e.g., simultaneous DDoS attack and account takeover).	
		IM:G2.Q4	Incident detection processes are capable of correlating events across the enterprise.	
	Advanced	CM:G1.Q1 CM:G2.Q1	Sophisticated and adaptive technologies are deployed that can detect and alert the incident response team of specific tasks when threat indicators across the enterprise indicate potential external and internal threats.	
		CM:G1.Q1 CM:G2.Q1	Automated tools are implemented to provide specialized security monitoring based on the risk of the assets to detect and alert incident response teams in real time.	Additional guidance—FFIEC requires support for real-time responses.
	Innovative	CM:G1.Q1 CM:G2.Q1	The institution is able to detect and block zero-day attempts and inform management and the incident response team in real time.	Additional guidance—FFIEC requires support for real-time responses.

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
RESPONSE AND MITIGATION	Baseline	IM:G4.Q1 IM:G4.Q2 IM:G4.Q3 IM:G4.Q4	Appropriate steps are taken to contain and control an incident to prevent further unauthorized access to or use of customer information. (FFIEC Information Security Booklet, page 84)	
	Evolving	IM:G1.Q1 IM:G2.Q5	The incident response plan is designed to prioritize incidents, enabling a rapid response for significant cybersecurity incidents or vulnerabilities.	Additional guidance—FFIEC requires that the incident response plan must include a prioritization of incidents.
		IM:G1.Q1	A process is in place to help contain incidents and restore operations with minimal service disruption.	
		IM:G3.Q3 IM:G4.Q2	Containment and mitigation strategies are developed for multiple incident types (e.g., DDoS, malware).	
		IM:G4.Q1 IM:G4.Q2 IM:G4.Q3	Procedures include containment strategies and notifying potentially impacted third parties.	
		IM:G3.Q2	Processes are in place to trigger the incident response program when an incident occurs at a third-party organization.	
		IM.G4.Q4	Records are generated to support incident investigation and mitigation.	
		EXD:G1.Q1 IM:G4.Q1	The institution calls upon third parties, as needed, to provide mitigation services.	
		IM:G5.Q2 IM:G5.Q3	Analysis of events is used to improve the institution's security measures and policies.	
	Intermediate	IM:G3.Q3	Analysis of security incidents is performed in the early stages of an intrusion to minimize the impact of the incident.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		CCM:G1.Q5 AM:G5.Q2 CCM:G2.Q8	Any changes to systems/applications or to access entitlements necessary for incident management are reviewed by management for formal approval before implementation.	
		AM:G6.Q6 CCM:G1.Q6	Processes are in place to ensure assets affected by a security incident that cannot be returned to operational status are quarantined, removed, disposed of, and/or replaced.	
		CCM:G2.Q7 SCM:G4.Q2	Processes are in place to ensure that restored assets are appropriately reconfigured and thoroughly tested before being placed back into operation.	
	Advanced	IM:G5.Q2 SA:G3.Q1	The incident management function collaborates effectively with the cyber threat intelligence function during an incident.	
		SA:G3.Q1	Links between threat intelligence, network operations, and incident response allow for proactive response to potential incidents.	
		IM:G3.Q3 IM:G4.Q2	Technical measures apply defense-in-depth techniques such as deep packet inspection and black holing for detection and timely response to network-based attacks associated with anomalous ingress or egress traffic patterns and/or DDoS attacks.	Additional guidance—FFIEC requires the use of these technical measures.
	Innovative	SCM:G1.Q6 RM:G2.Q4	The institution's risk management of significant cyber incidents results in limited to no disruptions to critical services.	
		Gap	The technology infrastructure has been engineered to limit the effects of a cyber attack on the production environment from migrating to the backup environment (e.g., air-gapped environment and processes).	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
Assessment Factor: Escalation and Reporting				
ESCALATION AND REPORTING	Baseline	IM:G3.Q3 IM:G4.Q1	A process exists to contact personnel who are responsible for analyzing and responding to an incident. (FFIEC Information Security Booklet, page 83)	
		IM:G4.Q3 IM:G2.Q8 IM:G2.Q9	Procedures exist to notify customers, regulators, and law enforcement as required or necessary when the institution becomes aware of an incident involving the unauthorized access to or use of sensitive customer information. (FFIEC Information Security Booklet, page 84)	
		IM:MIL4.Q3	The institution prepares an annual report of security incidents or violations for the board or an appropriate board committee. (FFIEC Information Security Booklet, page 5)	
		IM:G2 – all	Incidents are classified, logged, and tracked. (FFIEC Operations Booklet, page 28)	
	Evolving	IM:G3.Q1 IM:G4.Q1 IM:G4.Q2 IM:G4.Q3 IM:MIL3.Q1	Criteria have been established for escalating cyber incidents or vulnerabilities to the board and senior management based on the potential impact and criticality of the risk.	
		IM:G4.Q3	Regulators, law enforcement, and service providers, as appropriate, are notified when the institution is aware of any unauthorized access to systems or a cyber incident occurs that could result in degradation of services.	
		IM:G2.Q4	Tracked cyber incidents are correlated for trend analysis and reporting.	
	Intermediate	IM:MIL2.Q3	Employees that are essential to mitigate the risk (e.g., fraud, business resilience) know their role in incident escalation.	

Component	Maturity Level	CRR Reference	FFIEC Statement	Additions to CRR Question Guidance
		IM:G4.Q3	A communication plan is used to notify other organizations, including third parties, of incidents that may affect them or their customers.	
		IM:G4.Q2 IM:G4.Q3	An external communication plan is used for notifying media regarding incidents when applicable.	
	Advanced	IM:MIL4.Q1 IM:MIL4.Q2	The institution has established quantitative and qualitative metrics for the cybersecurity incident response process.	
		IM:MIL4.Q3	Detailed metrics, dashboards, and/or scorecards outlining cyber incidents and events are provided to management and are part of the board meeting package.	
	Innovative	IM:G4.Q1 IM:G4.Q3	A mechanism is in place to provide instantaneous notification of incidents to management and essential employees through multiple communication channels with tracking and verification of receipt.	Additional guidance—FFIEC requires instantaneous notification.

Bibliography/References

URLs are valid as of the publication date of this document.

[Caralli 2013]
Caralli, Richard & Butkovic, Matthew. Advancing Cybersecurity Capability Measurement Using the CERT-RMM Maturity Indicator Level Scale. CMU/SEI-2013-TN-028. Software Engineering Institute, Carnegie Mellon University. 2013. http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=69187

[DOE 2016]
Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2). *United States Department of Energy Website.* http://energy.gov/oe/cybersecurity-capability-maturity-model-c2m2-program/electricity-subsector-cybersecurity

[FFIEC 2015a]
Federal Financial Institutions Examination Council (FFIEC). *FFIEC Cybersecurity Assessment Tool—Overview for Chief Executive Officers and Boards of Directors).* June, 2015. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_CEO_Board_Overview_June_2015_PDF1.pdf

[FFIEC 2015b]
Federal Financial Institutions Examination Council (FFIEC). *FFIEC Cybersecurity Assessment Tool User's Guide.* June, 2015. https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_User_Guide_June_2015_PDF2_a.pdf

[FFIEC 2016a]
Cybersecurity Assessment Tool (CAT). *Federal Financial Institutions Examination Council (FFIEC) Website.* https://www.ffiec.gov/cyberassessmenttool.htm

[FFIEC 2016b]
FFIEC IT Examination Handbook InfoBase Glossary. *Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook InfoBase Website.* http://ithandbook.ffiec.gov/glossary.aspx

[NIST 2014]
National Institute of Standards and Technology. *Framework for Improving Critical Infrastructure Cybersecurity.* February 12, 2014. http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf

[SEI 2016]
CERT-RMM. *Carnegie Mellon University Software Engineering Institute Website.* http://www.cert.org/resilience/products-services/cert-rmm/index.cfm

[US-CERT 2016]
Assessments: Cyber Resilience Review (CRR). United States Computer Emergency Readiness Team (US-CERT) Website. https://www.us-cert.gov/ccubedvp/self-service-crr

[WH 2013a]
Presidential Policy Directive—Critical Infrastructure Security and Resilience. *The White House, Office of the Press Secretary Website.* February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[WH 2013b]
Executive Order 13636—Improving Critical Infrastructure Cybersecurity. *The White House, Office of the Press Secretary Website.* February 12, 2013. https://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
(Leave Blank)	October 2016	Final

4. TITLE AND SUBTITLE	5. FUNDING NUMBERS
A Mapping of the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the Cyber Resilience Review (CRR)	FA8721-05-C-0003

6. AUTHOR(S)

Jeffrey L. Pinckard, Michael Rattigan, Robert A. Vrtis

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	CMU/SEI-2016-TN-008

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSORING/MONITORING AGENCY REPORT NUMBER
AFLCMC/PZE/Hanscom Enterprise Acquisition Division 20 Schilling Circle Building 1305 Hanscom AFB, MA 01731-2116	n/a

11. SUPPLEMENTARY NOTES

12A DISTRIBUTION/AVAILABILITY STATEMENT	12B DISTRIBUTION CODE
Unclassified/Unlimited, DTIC, NTIS	

13. ABSTRACT (MAXIMUM 200 WORDS)

This technical note describes the methodology we used and the observations we made while mapping the declarative statements found in the Federal Financial Institutions Examination Council (FFIEC) Cybersecurity Assessment Tool (CAT) to the practice questions found in the US-CERT Cyber Resilience Review (CRR). This mapping enables financial organizations to use CRR results not only to gauge their cyber resilience, but to examine their current baseline with respect to the FFIEC CAT and the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The mapping in this technical note is proposed by three senior engineers from the CERT Division of the Carnegie Mellon University Software Engineering Institute; these engineers are skilled in conducting CRRs and familiar with all practice questions and question guidance. Two also have the advantage of several years of experience in the financial sector. The team relied on their experience along with previous mappings of the CRR and FFIEC CAT to the NIST CSF to propose the mapping in this technical note.

14. SUBJECT TERMS	15. NUMBER OF PAGES
CRR, FFIEC, CAT, cybersecurity	82

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89) Prescribed by ANSI Std. Z39-18
298-102