The Expanded Scope of the Compliance Management System – Information Technology

DECEMBER 2021

AUTHORS:

Paul Noring
202.839.3925
pnoring@thinkbrg.com

Vincent Urbancic
202.480.2752
vurbancic@thinkbrg.com

INTELLIGENCE THAT WORKS

BRG

The Consumer Finance Protection Bureau's (CFPB) created its compliance management system (CMS) to support financial institutions in maintaining regulatory compliance. The integration of CMS into the business strategies of financial institutions ensures their establishment and the communication of compliance responsibilities; incorporation of these responsibilities into business processes; review of operations to ensure fulfillment of compliance requirements; and review, correction, and adaptation of new systems and tools, as necessary.[1] Both the CMS and the new *Compliance Management Review (CMR-IT)* include five modules: Board and Management Oversight, Compliance Program, Service Provider Oversight, Violations of Law and Consumer Harm, and Examiner Conclusions and Wrap-Up.[2]

The CFPB, with the September 2021 release of the Information Technology section of its examination manual, aims to oversee the impact that an institution's information technology has on compliance with federal consumer laws. The IT examination procedures allow the CFPB and financial entities to evaluate the technological controls of an entity and its service providers as part of their overall CMS.[3]

Numerous enforcement actions have been associated with deficiencies in the CMSs of institutions. The CFPB also has published articles on the importance of CMS. One recent example is the June 2021 supervisory highlights, which mention CMS seven times, highlighting its importance to the CFPB.[4] Institutions within the scope of the CFPB supervision should pay attention to these new assessments.

1 CFPB, *Examination Procedures: Compliance Management Review* (updated August 2017). https://files.consumerfinance.gov/f/documents/201708_cfpb_compliance-management-review_supervision-and-examination-manual.pdf

2 Ibid.

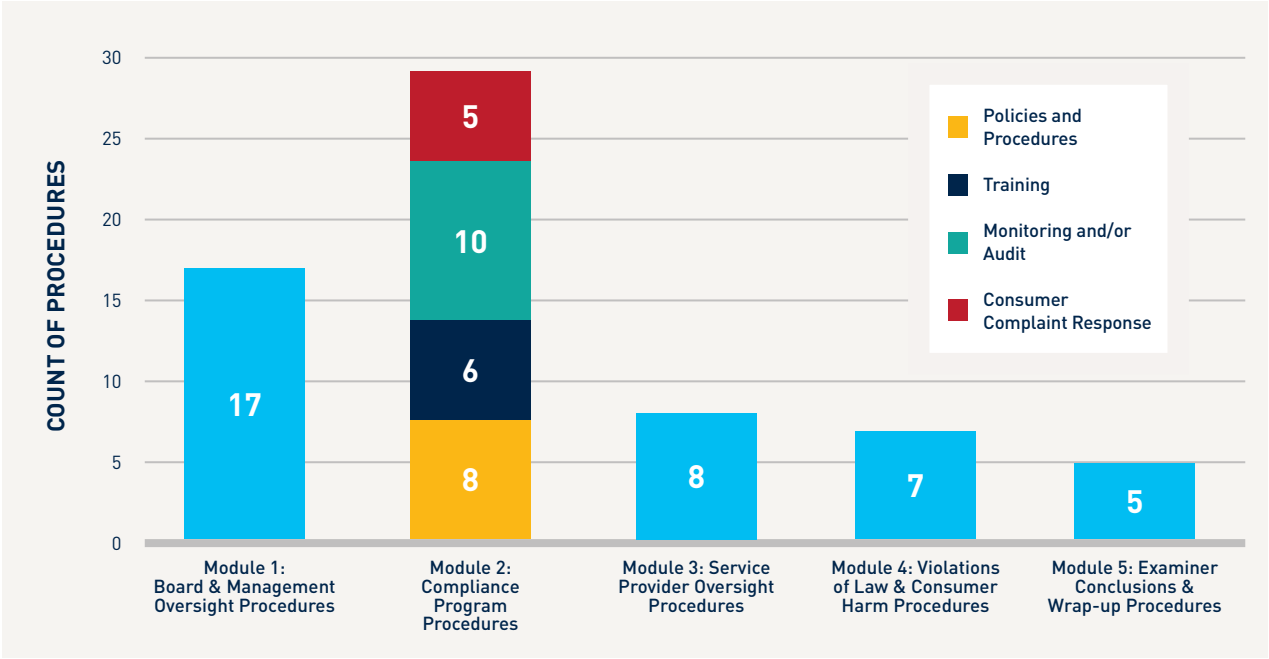
3 CFPB, *Examination Procedures: Compliance Management Review – Information Technology (CMR-IT)* (September 2021). https://files.consumerfinance.gov/f/documents/cfpb_compliance-management-review-information-technology_examination-procedures.pdf

4 CFPB, *Supervisory Highlights, Issue 24, Summer 2021* (June 2021). https://files.consumerfinance.gov/f/documents/cfpb_supervisory-highlights_issue-24_2021-06.pdf

CMR-IT

Similar to the previous CMR, the CMR-IT is divided into objectives and procedures. The objectives outline the components required of each section, while the procedures provide steps on how to evaluate whether the entity has met the objectives. Figure 1 shows the number of CMR-IT procedures by each of the pillars of the CMS.

Figure 1. Number of Objectives and Examination Procedures in CMR-IT[5]



Module 1: Board and Management Oversight – IT section

The examination of this module includes ensuring appropriate oversight of and commitment to the institution's CMS. This module studies the board of directors' and senior management's interactions with and oversight of the IT workforce, as well as security policies and procedures in place. The examination procedures target identifying and evaluating inherent risks related to IT, retaining organized records of IT risk assessment findings, overseeing controls around the system development life cycle (SDLC), ensuring that the IT change management process aligns with the entity's IT risk appetite, and establishing an ongoing and process-oriented approach to business continuity planning.[6]

5 Based on BRG analysis of CFPB, *CMR-IT* (2021).
6 CFPB, *CMR-IT* (2021).

Module 2: Compliance Program

The Compliance Program consists of the following elements:

1. Policies and procedures
2. Training
3. Monitoring and/or audit
4. Consumer complaint response

1. *Policies and procedures:* This element seeks to validate that the institution's compliance policies and procedures adhere to board-approved compliance policies and federal consumer financial laws. Also, it seeks to verify whether these policies are continuously being updated and effectively address IT controls and compliance risk in the products, services, and activities of the institution.
2. *Training:* This element evaluates the effectiveness of the IT security training program by validating the existence of a security awareness training program for all employees and reviewing policies and training evidence for role-based training of IT staff and service providers with IT responsibilities. It also involves a review of records of follow-up, escalation, and enforcement of training completion rates that do not meet the supervised entity's standards; and the analysis of future IT training plans.
3. *Monitoring and/or audit:* This element examines the quality of IT audit oversight and whether the entity has an independent audit function; and evaluates monitoring/audit policies and procedures and whether they incorporate compliance with federal consumer financial laws.
4. *Consumer complaint response:* This element assesses how well the entity identifies, reviews, escalates, and resolves IT-related consumer complaints and inquiries about the entity and its service providers. Also, it examines whether the institution has the necessary policies and procedures in place for this process to occur. Moreover, the examination procedures evaluate whether corrective actions applied for IT-related complaints result in a violation of the relevant laws and regulations.[7]

Module 3: Service Provider Oversight

This module focuses on evaluating the relationships with service providers that support the institution's IT functions, especially those that have access to sensitive information. It validates whether these service providers are being assessed and monitored and the effectiveness of oversight. Also, this module reviews policies and procedures that the institution has in place for application or system acquisition activities and the risk management program for service-provider oversight that support IT functions.[8]

Module 4: Violations of Law and Consumer Harm

The objective of this module is to identify the types and severity of the IT-related weaknesses in the institution's CMS. It scrutinizes whether entities self-identify violations, determine the root cause of violations, and evaluate their impact on consumers. Also, this module addresses the effectiveness of the implemented corrective measures for a given set of violations.[9]

7 CFPB, CMR-IT (2021).
8 Ibid.
9 Ibid.

Module 5: Examiner Conclusions and Wrap-Up

This module seeks to identify and discuss, with the institution's management, the findings and/or concerns for each of the modules completed in the review and implement remediation actions as needed. It involves keeping a record of findings according to CFPB policy in the examination report/supervisory letter and preparing a memorandum for the CFPB.[10]

Key Differences between CMR and CMR-IT

In contrast with the CMR, which focuses on examining the enterprise-wide compliance management system, the CMR-IT takes a closer look at the information technology used by financial institutions and how it can impact compliance with federal consumer financial laws. Taking the two manuals at face value is not a one-to-one comparison. Rather, they are two separate reviews: even though the entity may have performed a CMS review does not mean it can ignore the new CMR-IT. Table 1 represents the number of procedures in, and the differences between, the CMR and the CMR-IT.[11]

Table 1. Number of Procedures Comparison and Key Differences[12]

Area	Module 1: Board & Management Oversight	Module 2: Compliance Policies and Procedures	Module 2: Compliance Training	Module 2: Compliance Monitoring	Module 2: Compliance Consumer Complaint Response	Module 3: Service Provider Oversight	Module 4: Violations of Law & Consumer Harm	Module 5: Examiner Conclusions & Wrap-Up
CMR – August 2017	16	13	10	20	15	7	7	5
CMR IT - September 2021	17	8	6	10	5	8	7	5
Difference in # of Procedures	1	(5)	(4)	(10)	(10)	1	0	0
Key Area of CMR-IT	Evaluates board of directors' and senior management's interactions with and oversight of the IT workforce and the security policies and procedures in place.	Analyzes structure of the consumer compliance program and how it interacts with IT functions and controls to ensure compliance with federal consumer financial laws.	Validates that there is an established IT security training program for all employees, as well as IT role-based training for IT staff and service providers that perform IT functions.	Examines the IT audit oversight an entity can provide, including whether the entity has an independent audit function or if IT audits are performed by a third party.	Assesses how well the entity identifies, reviews, escalates, and resolves IT-related consumer complaints and inquiries about the entity and its service providers about its size, complexity, and risk profile.	Reviews the entity's monitoring and oversight policies and procedures related to service providers that support the institution's IT functions.	Verifies whether the institution determines the root cause of violations due to the use of IT, and evaluates the impact on consumers.	Summarizes and discusses findings from previous modules, identifies needed remediation actions, and creates a record of findings.

10 Ibid.
11 Ibid.
12 Based on BRG analysis of CFPB, *CMR-IT* (2021).

Conclusions

The CMS is no longer just a review for standard compliance operations, but rather has a new focus. The CMR-IT takes a deep dive into the world of technology that supports compliance and risk functions. Most recently, the CFPB announced an inquiry into six Big Tech payment platforms and a study of two Chinese payments platforms.[13] We project similar inquiries will start happening with smaller entities, based on recent attempts by Congress to rein in the power of Big Tech and CFPB Director Rohit Chopra's reputation as a consumer advocate who is frequently tough on technology companies. Institutions would be prudent to incorporate the new CMR-IT objectives and procedures into their compliance management review assessments.

13 Michael Canale and Vincent Urbancic, *The Chopra CFPB Arrives with a Warning to Big Tech,* BRG (November 1, 2021). https://www.thinkbrg.com/insights/publications/chopra-cfpb-big-tech/

About BRG

Berkeley Research Group, LLC (BRG) is a global consulting firm that helps leading organizations advance in three key areas: disputes and investigations, corporate finance, and performance improvement and advisory. Headquartered in California with offices around the world, we are an integrated group of experts, industry leaders, academics, data scientists, and professionals working beyond borders and disciplines. We harness our collective expertise to deliver the inspired insights and practical strategies our clients need to stay ahead of what's next. Visit thinkbrg.com for more information.

THINKBRG.COM